Amadeus 5

Basic User Manual

Publication No. 18UE401 V2011 © DDS 2011

DDS
Building Security Together

About this Basic User Manual:

This Basic User Manual describes the general functioning of Amadeus5 software, how to install it and how to define the basic functions. Full updated features are available in your Amadeus5 installation CD and on the software Help, accessible directly from the application. (See the ‘Help’ chapter)

Table of Contents

1 Application Overview 5
1.1 About Amadeus 5
1.2 Copyright and Trademarks 6
1.3 Basic Functions and Optional Modules 6
1.4 Application Basic Functions 7
1.4.1 Access Control 7
1.4.2 Alarm Control 8
1.4.3 Basic Time and Attendance 8
1.4.4 Report Wizard 8
2 Quick Guide 9
2.1 Setting up the Application 9
2.1.1 Installation Types 9
2.1.2 Configuration 9
2.1.3 Software Requirements 10
2.2 Getting Started 10
2.2.1 Demonstration Version 10
2.2.2 Installation of the Application (New or update) 11
2.2.3 Running the Appplication 11
2.2.4 Application Information 12
2.2.5 Force Local and Remote Restart/Shutdown 13
2.2.6 Update an Application version 13
2.3 Application User Interface 14
2.3.1 Application Bar 14
2.3.2 Menu Ribbon 15
2.3.3 Toolbar 15
2.3.4 Log Window 15
2.3.5 Data Toolbar 16
2.4 Accessing Help from the Application 17

3 Parameter Tab 18
3.1 Computer 18
3.2 Controller Network 19
3.2.1 Controller Network / General 19
3.2.2 Controller Network / Definition 19
3.2.3 Updating Remote (Dial-up) Controllers via the Modem 22
3.3 Controller 23
3.3.1 Controller / General 24
3.3.2 Controller / Readers 25
3.3.3 Controller / Input 33
3.3.4 Controller / Output 35
3.3.5 Controller / Local Reflexes 37
3.4 Time Zone 39
3.4.1 Daily Programme 39
3.4.2 Weekly Programme 40
3.4.3 Holiday 42
3.5 Access Group 43
3.6 Department 44
3.7 Badge 45
3.7.1 Using the Badge Search 46
3.7.2 Create / Delete a Group of Badges 47
3.8 Cardholder 49
3.8.1 Cardholders / General 49
3.8.2 Cardholders / Personal Tab 53
3.8.3 Cardholders / Location Tab 54
3.8.4 Cardholders / Customized Tab 55
3.8.5 Cardholders / Exceptions Tab 55
3.8.6 Cardholders / Schedule AG Tab 56
3.8.7 Cardholders / Vacations Tab 56
3.8.8 Cardholders / Attached Documents 57
3.9 Visitor 58
3.10 Authorization Levels 58
3.11 User 59
3.12 Customized Labels and Customized Fields 60

4 Event Handling Tab 61
4.1 Event Handling Programme / Alarms 61
4.2 Event Handling Programme / Alarm Properties Window 63
5 Communication Tab 65
5.1 Diagnostic 65
5.1.1 Diagnostics – Controller Information 65
5.1.2 Diagnostics / Menu 67
5.2 View / Clear Log 67
6 View Tab 68
6.1 Display Photo 68
7 Tools Tab 69
7.1 Report Wizard 69
7.1.1 Report Wizard Step 1/4 – Report Selection 69
7.1.2 Report Wizard Step 2/4 – Data Selection 72
7.1.3 Report Wizard Step 3/4 – Data Filtering 74
7.1.4 Report Wizard Step 4/4 – Data Organization 75
7.2 Other Available Tools 76
8 Help Tab 77
8.1 Help Contents 77
8.2 Help Index 77
8.3 Help Search 77
8.4 Web 77
8.5 About 77

1 APPLICATION OVERVIEW

1.1 ABOUT AMADEUS

Amadeus5 is a sophisticated yet user-friendly security platform which transforms your facility into a smart building. It is built around specialized modules, with each covering a specific branch of the security such as access control, alarm management, video monitoring, parking management, guard tours, lift control, time & attendance etc. All these modules provide centralized security control for all types of installations irrespective of their complexity.

The modular and scalable system capacity can handle effectively unlimited numbers of all entities in each branch of the security - cardholders, controllers, readers, supervised alarms, outputs, video servers, operators, access groups, security levels, etc. The system can be used by a single company, shared by several tenants located in the same building or a multi-building complex, and offers solutions suitable even for international companies with offices spread over the world.

The user-friendly software is easy to configure and use, with predefined parameters for fast installation, automatic actions and reflexes as well as a personalized report wizard. Full information on real time alarms and events is provided in an active alarm window and live interactive graphical maps, in the event log, and on diagnostic screens.

The user screen provides all necessary information to react immediately, with full knowledge of the facts. Security is reinforced as alarm conditions and events automatically trigger predefined reactions: flashing icons on relevant displayed maps, message displays and playback of verbal instructions, alarms, CCTV or any programmed relay activation, setting alarms on/off by zone, card invalidation, etc.

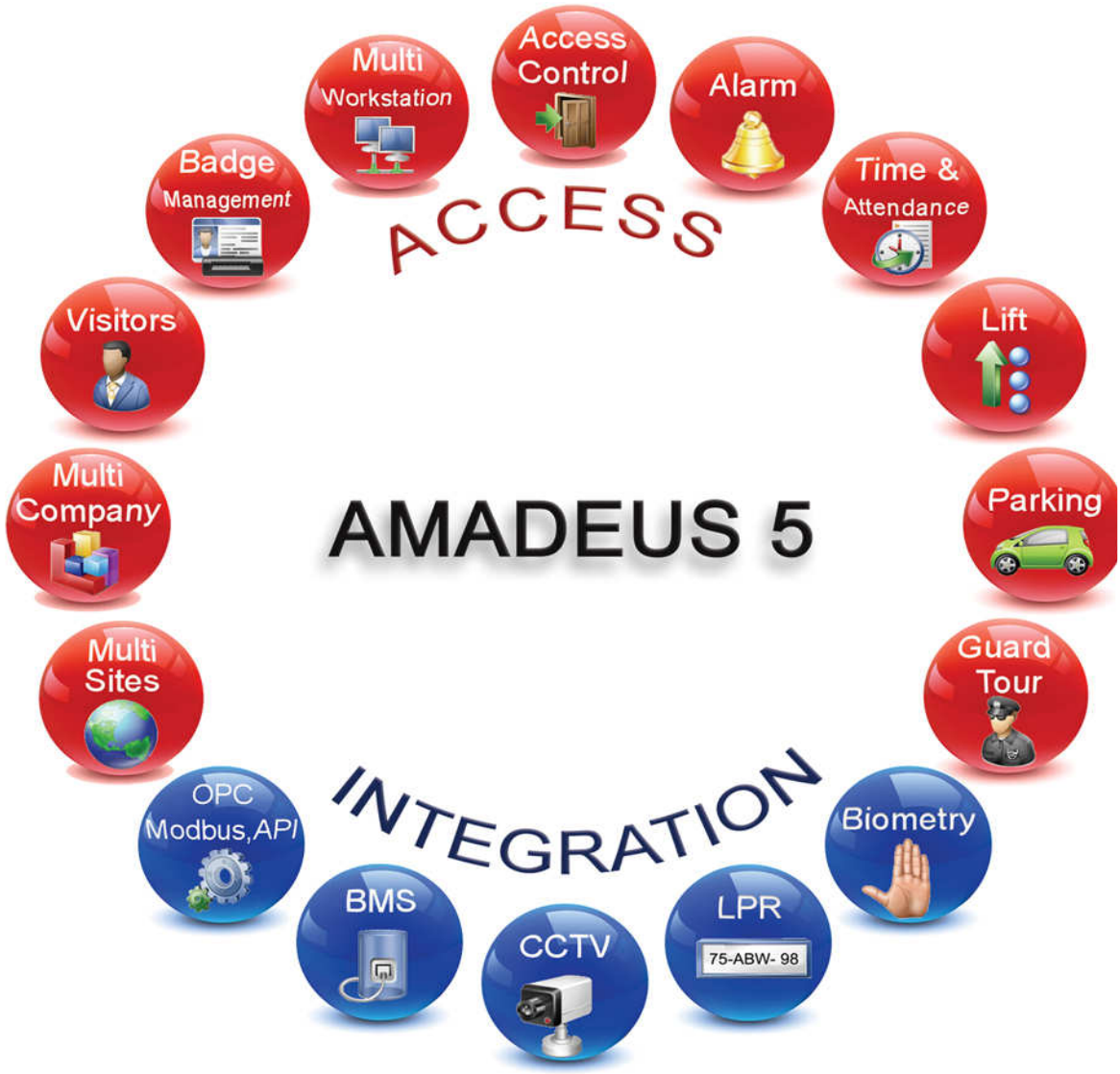
Sets of Actions (‘Processes’) can be defined and invoked by the system or manually.

The Amadeus5 application (‘the Application’) consists of a powerful core of standard capabilities (Access Control, Alarm Control, T&A, Report Wizard) and a versatile range of optional modules for users with particular requirements. These include specific integrations allowing users to combine the Application’s comprehensive Access Control system with specialist functionality incorporating the latest technologies available in the market.

1.2 COPYRIGHT AND TRADEMARKS

- Microsoft, Windows .NET and Visio are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Intel, Pentium and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.
- Spread Toolkit is either a registered trademark or trademark of Spread Concepts LLC in the United States and/or other countries.
- NetHASP is either a registered trademark or trademark of Aladdin Knowledge Systems Ltd. in the United States and/or other countries.

1.3 BASIC FUNCTIONS AND OPTIONAL MODULES



1.4 APPLICATION BASIC FUNCTIONS

1.4.1 ACCESS CONTROL

The system supervises the access to all or part of your facility (offices, production areas, lab, computer room, or storage areas) by authorized persons, during user-defined time periods. Smart multi-technology controllers, linked to advanced readers, are programmed to control "who is going where and when".

Each **Controller** has its own large memory capacity so that the entire database relevant to the access points connected to that controller is recorded locally. Controllers store the list of cardholders authorized at its **Readers** and their time parameters, and also the time parameters applicable to readers, how the doors are to be controlled, and all the access rules to be enforced, including special rules for holidays, whether an escort is required, whether Anti-Passback is to be applied, and so on.

Cardholders - All authorized personnel (staff, contractors and visitors) have personalized **Badges** that control their access. These can include card or other ID methods (including advanced ID systems such as biometrics).

When cardholders attempt to access a particular area by using their badge or other ID at a reader, the information is relayed to the reader’s controller. Access checking is performed instantly (no need for PC intervention), and access is granted or refused by applying the parameters relevant to the cardholder and the reader at that time. The resulting transactions are sent to the PC where they are displayed, stored in the **System Log** and are available for later reporting.

Additional routine information about cardholders, such as photo, address, phone number, car registration and so on, can be stored, and custom information may be added. All information is available for the operator as queries, and may be included in reports.

Badges - A comprehensive range of industry-standard identification methods are supported, including Wiegand, magnetic and barcode cards, as well as biometric identification. Provision is made for a wide variety of formats and variations, and more than one type/format can be supported within a single installation – this can be vital where organizations merge, or where different organizations share facilities within one set of premises.

1.4.2 ALARM CONTROL

Alarm Management - Your organization can prevent catastrophes or limit damage by being informed of abnormal events and reacting to them in real time. The system supervises **Alarm Inputs** from sensors at predefined alarm points. Examples of sensors may be magnetic contacts, motion detectors, door and window sensors and temperature indicators. These are connected to **Inputs** on intelligent **Controllers,** and their status can be monitored and reported centrally. The system can be set to react to alarm inputs by opening or closing **Relays** (or '**Outputs'**) that control doors, activate audible alarms, light alarm panels, or operate air-conditioning and other equipment. Local Reflexes allow the status of an Input to be used directly as the trigger for an Output. Thus, a 'door open' sensor can trigger a local warning light or audible alarm.

Site Scheduling – The system allows definition of Time Zones which define when particular sets of rules must be applied. Time zones are grouped into **Daily** and **Weekly Programmes** that define when the rules must be applied for readers, alarms and cardholders.

1.4.3 BASIC TIME AND ATTENDANCE

The system provides accurate recording of either start- and end-times or a full list of all clockings. This reduces queries and allows more efficient calculation of pay slips.

1.4.4 REPORT WIZARD

A sophisticated Report Wizard provides predefined reports on all elements of the system, and allows the user to add or remove categories of information and filter the data to produce more specific, customized reports where required. Reports cover all types of system transactions, and can also list hardware information and configuration parameters.

A preview facility allows the user to see what a particular set of parameters will produce before actually printing the report. The user can then return to the parameter screens and make further modifications until the required report is built.

New user report definitions may be stored so that the tailored reports are 'named' and can be called later and re-used without requiring re-definition.

2 QUICK GUIDE

2.1 SETTING UP THE APPLICATION

2.1.1 INSTALLATION TYPES

The Application provides centralized on-line security control within any type of installation:

- Big or small installation
- TCP/IP, RS485 or modem networks
- Central or dispersed locations
- Single-company or shared multi-company sites

2.1.2 CONFIGURATION

The Application software can run on a standard Windows® PC with the following minimum configuration:

Operating system

Windows 7®, Vista®, Windows XP Pro®
Windows Server 2003®
Windows Server 2008® (supported from version 2.1)

Computer

Pentium® IV
256 MB RAM
(or 1 GB RAM for installations over 100 controllers or with SQL Server)
Compatible with 32-bit or 64-bit processors
500 MB free hard disk space
CDROM Drive
1 free serial COM port for communication or a network card for TCP/IP
USB port

Recommended enhancements

Sound Card
Speakers
SVGA definition (800*600)

Controllers

Wide range of compatible proprietary controllers is available.

Readers

The vast majority of readers available on the market are compatible with the controllers that are supplied with the system: magnetic, proximity, bar code, smart card, biometry, Wiegand, contact, infrared, Watermark, keypad, etc.

Other Components

In order to successfully install and run the Application, other materials are required. These vary according to each installation: computer network, devices to open doors, alarm detectors, etc

Consult with your reseller for further information.

2.1.3 SOFTWARE REQUIREMENTS

.NET FRAMEWORK

This version requires Microsoft® .NET connection software version 2.0. If it is not already installed on the PC, it is available for download from Microsoft at:

http://www.microsoft.com/downloads/details.aspx?familyid=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en

INTERNAL MESSAGING SOFTWARE

The system uses software developed by Spread Concepts LLC for use in the Spread toolkit. For more information about Spread see http://www.spread.org.

NETHASP SUPPORT FOR TERMINAL SERVER APPLICATION COMPATIBILITY

The Application can work either from a Terminal Server PC or from a Terminal Client. However, this requires a NetHasp® dongle to enable the Terminal application. The Terminal Client workstation normally looks for the installed dongle on the PC. The special NetHasp dongle (coloured red for quick identification), can be physically installed on the Server or on any other PC on the LAN, and is read by the Application through the network.

2.2 GETTING STARTED

2.2.1 DEMONSTRATION VERSION

A demo version of the Application software is available, allowing prospective users to work with the application, try out the user interface, and see details of all the data fields that are available.

Running the demo version gives access to all functions including alarms, graphics, lift management and time management but it supports only a limited set of devices - two controllers, four readers and ten cardholders.

To run the demo, start the programme without using a dongle, and enter the username and password ‘dds’. In order to exceed the demo capabilities and to use the software in a real situation, the software must be licensed and a dongle installed.

2.2.2 INSTALLATION OF THE APPLICATION (NEW OR UPDATE)

Insert the Application Installation CD: the Installation Wizard is automatically launched. If the Wizard does not start by itself, run the 'autorun.exe' file in the 'autorun' folder of the Installation CD. Follow the step by step instructions.

Setup - Amadeus 5
Welcome to the Amadeus 5 Setup Wizard
This will install Amadeus 5 version 2.1.534 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

Note: Do not install the application using the 'setup.exe' file of the CD; should you do so, the following warning message will be displayed:

Setup will not start. Contact your vendor

Application Type: If the application runs on one computer only, select 'Server' as the Application Type. If on several computers (i.e. Server/Workstations architecture), do as follows:

- Install the application on the computer that will be the Server and specify 'Server' during the installation process
- Share the Application folder to the required Workstation(s)
- Once installed, run the application and define all the computers, Server and Workstation(s), through the Computer screen
- Install the application on each workstation and specify 'workstation' during the installation process. It will ask the user to select the Server network path

2.2.3 RUNNING THE APPPLICATION

Start the application by double-clicking on its shortcut or by clicking on Start/Programs/<Application>/<Application> from Windows Desktop.

Type the User name and Password and click OK.

Default values for first use are: Username: DDS Password: DDS

These values should be changed on first use, and the new values stored in a secure place.

The application main menu appears on the screen.

Notes:

Significance of lower case and capital letters: The "User name" and "Password" fields are case-sensitive. For example: the computer will interpret AFI, afi, and aFi differently.

Three attempts: If the user name and the password are not correctly entered after three attempts, the start window will disappear from the screen.

To skip the user name and password request: To start your application without being prompted for a user name and a password every time the application is started, set them in the initialization parameters, as follow:

Point the mouse to the shortcut of the application
Right click on the application icon
Select “Properties”
Add the user name and password at the end of the “Target” field
(after “<Application>.exe”) as follows

[space]/us:user name [space]/pw:password

Click OK

2.2.4 APPLICATION INFORMATION

During startup, the application splash screen is shown, with the following information:

Version: The specific version number

User ID: The license ID stored in the dongle

License: Details of configuration limits and all the modules for which licenses have been provided

Configuration limits:

nC Maximum No. ('n') of Controllers allowed
nR Maximum No. ('n') of Readers allowed
nB Maximum No. ('n') of Cardholders allowed
nW Maximum No. ('n') of Workstations allowed (not shown in Demo mode)
LIGHT Pre-configured “Light” version

Modules Licensed:

A Alarm Module
G Basic Graphics Module
P Parking Module
L Lift Module
T Basic Time & Attendance Module
U Guard Patrol
M Multi Company
O OPC Server
SQL SGL Server
BP Badge Printing Module
V Video Module
Modbus Modbus TCP
nMS Multi-site (‘n’=sites number)
G+ New Graphics + Module
T + Time & Attendance + Module
LPR License Plate Recognition Module

Startup Progress: During installation the progress bar is shown as a bar. The milestones shown below the bar indicate the specific components being processed.

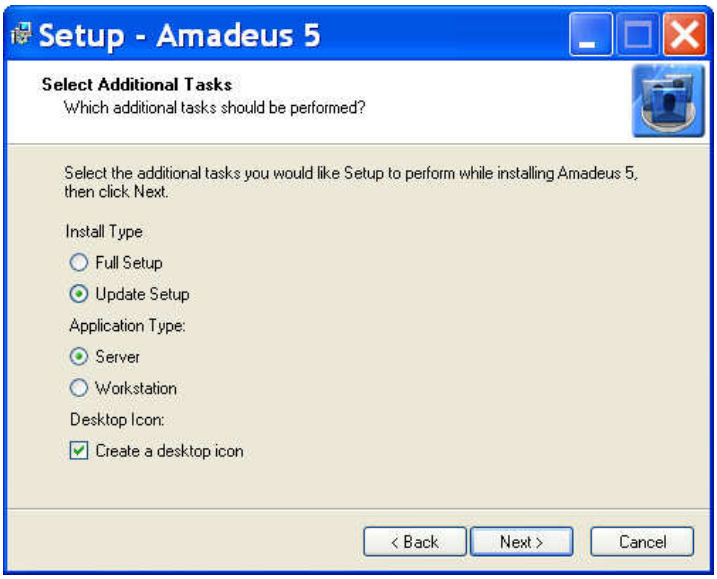
2.2.5 FORCE LOCAL AND REMOTE RESTART/SHUTDOWN

From the Application Menu screen, select ‘Parameter’ and then ‘Computer’. Once in the ‘Computer’ screen, press Shift/F12. Two buttons are shown, enabling **Restart** or **Shutdown** of any Application instance. The operation is executed through the database, and thus Remote Restart / Shutdown will work even when the **Spread** application is down.

> **Important**: The requests are NOT performed immediately. There can be up to 1 minute delay from the request till the Restart / Shutdown is performed on the relevant Application instance.

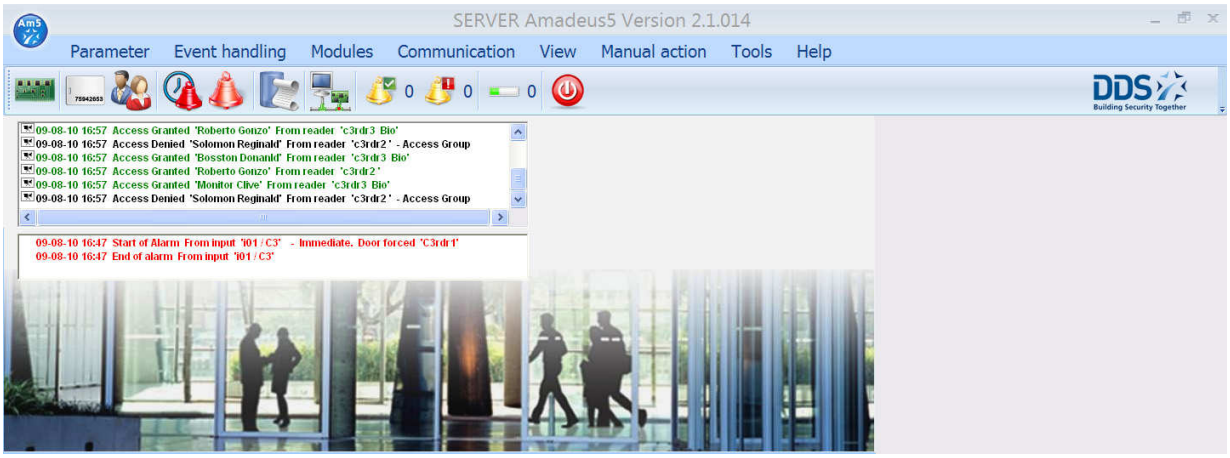
2.2.6 UPDATE AN APPLICATION VERSION

To update an existing application, run the new version installation CD. When the ‘Set-up - Amadeus 5’ screen appears, select the ‘Update setup’ option.



2.3 APPLICATION USER INTERFACE

The Application provides a simple, powerful user interface.


SERVER Amadeus5 Version 2.1.014
Parameter
Event handling
Modules
Communication
View
Manual action
Tools
Help
09-08-10 16:57 Access Granted 'Roberto Gonzo' From reader 'c3rdr3 Bio'
09-08-10 16:57 Access Denied 'Solomon Reginald' From reader 'c3rdr2' - Access Group
09-08-10 16:57 Access Granted 'Bosston Donanld' From reader 'c3rdr3 Bio'
09-08-10 16:57 Access Granted 'Roberto Gonzo' From reader 'c3rdr2'
09-08-10 16:57 Access Granted 'Monitor Clive' From reader 'c3rdr3 Bio'
09-08-10 16:57 Access Denied 'Solomon Reginald' From reader 'c3rdr2' - Access Group
09-08-10 16:47 Start of Alarm From input 'I01 / C3' - Immediate, Door forced 'C3rdr1'
09-08-10 16:47 End of alarm From input 'I01 / C3'

2.3.1 APPLICATION BAR

The top line of the Application window indicates whether this is the SERVER or a WORKSTATION, and shows the Application name and version number.

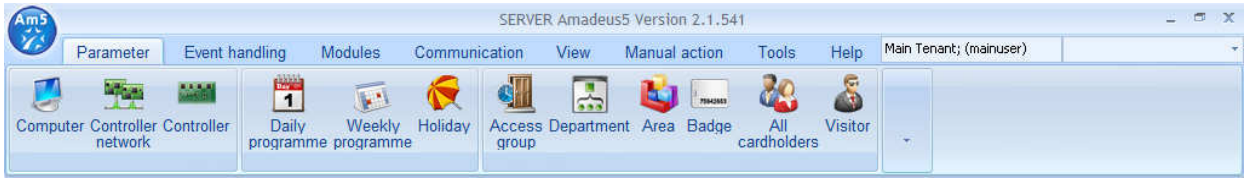
Clicking on the **Application icon** opens an Operator menu.
Change Password: Operator can change the password.
Log off: Logs the current user off. A new logon is required.

Exit: Exits the application

Notes:

- The ini file entry PasswordExpireAfter_Days = n
  will make the User enter and confirm a new password after n days
- The ini file entry AllowReuseUserPassword=0
  prevents the User from re-using a password**.**

2.3.2 MENU RIBBON

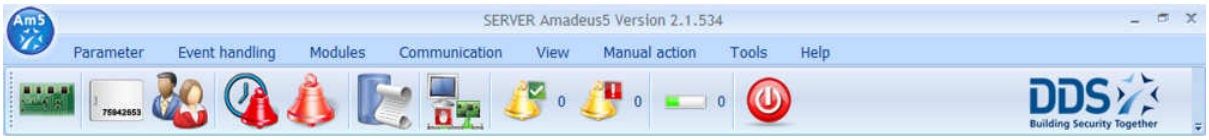


The Menu Ribbon has 8 pull-down tabs, each with set of entries, grouped into related functions. Clicking on a tab opens the detailed Menu Ribbon for that tab function.
Double-clicking on the Tab will keep the detailed Menu Ribbon visible even after a selection is made. Double-clicking on the tab a second time will minimise it again.

Note: The options displayed depend on the specific licensed options, and on the authorization level of the operator.

Where a low-resolution screen or a partial screen window is used for the main screen, the Main Ribbon is shortened, and a **pulldown button** must be clicked to open the additional tabs.

2.3.3 TOOLBAR



The Toolbar provides access to **frequently-used functions**, shows the **status of communication** with Controllers, and indicates the number of **current and outstanding Alarm Events**.

2.3.4 LOG WINDOW

09-08-10 16:57 Access Granted 'Roberto Gonzo' From reader 'c3rdr3 Bio'
09-08-10 16:57 Access Denied 'Solomon Reginald' From reader 'c3rdr2' - Access Group
09-08-10 16:57 Access Granted 'Bosston Donanld' From reader 'c3rdr3 Bio'
09-08-10 16:57 Access Granted 'Roberto Gonzo' From reader 'c3rdr2'
09-08-10 16:57 Access Granted 'Monitor Clive' From reader 'c3rdr3 Bio'
09-08-10 16:57 Access Denied 'Solomon Reginald' From reader 'c3rdr2' - Access Group

The log window is a dynamic display that shows system events as they occur. The types of events to be displayed (and to be saved in the Journal) and the default colours for different types of entries (red for alarms, green for access granted, black for access denied, etc.) are given in Tools/Options/Menu screen

The Log window scrolls upwards, with new events inserted at the bottom in the sequence in which they occur.

The Log window can be hidden/shown, and the Log can be cleared, using the corresponding buttons in the Communications tab.

The user may wish to 'freeze' the display so that particular events remain visible even though other events are taking place that would cause the window to scroll.

Setting the .ini option **ScrollLogs = 1** adds '**On'** and '**Off'** scroll buttons above the log window. Clicking on these buttons freezes/unfreezes scrolling of the Log.

2.3.5 DATA TOOLBAR

All data screens have a common set of icons, and support a common set of Function Keys as follows:

Key	Function	Description
F1	Help	Display Help information about the current screen
F2	New	Define a new data entry.
F3	Save	Save the current data. Updates the relevant database.
F4	Delete	Delete the selected data entry
F5	First	Select the first data entry of the list
F6	Previous	Select the previous data entry
F7	Next	Select the next data entry
F8	Last	Select the last data entry of the list
F9	Download	Transfer all the parameters to the corresponding controllers even if the information has not been modified
F10	Search	Lists all records that match the information entered into any of the fields
F11	Print	Automatically generate the report corresponding to the current data entry
F12	Close	Close the current screen

Tabs: Several Data Windows have additional Tabs for specific information. Clicking on a Tab changes the Data Pane to display the information for the selected tab, and highlights the selected data record in the Navigation Pane.

Navigation Pane: The list of existing records for the selected data type is shown, in alphabetical order. When an item is selected by clicking on it, the relevant data record is shown in the Data Pane.

Data Pane: The Data Pane displays all the information for the selected item. Click **New** to enter a new record.

Note: In complex screens, such as **Cardholder** or **Controller**, the identifying information (i.e. 'Name' in the case of Cardholders, etc.) must be entered and then **Saved**, before the rest of the new data can be entered.

2.4 ACCESSING HELP FROM THE APPLICATION

Most screens in the system are linked directly to their own Help pages (accessed by pressing F1 from the Application screen). Where specific screens do not have their own links, Help material is accessible from the Table of Contents in the left panel of the Help window. The **Search** button displays all topics that refer to the item in the Search window, and the Search Window includes options to search for titles only, similar words, or limiting the search to previous search results. All targets words are highlighted.

3 PARAMETER TAB

The Parameter Tab displays the screens associated with setting up the system.

When a new item is created (controller, reader, cardholder, etc.), the system creates most of the parameters with standard default values, using standard practices established for the system in the field. The user may change these values where required.

3.1 COMPUTER

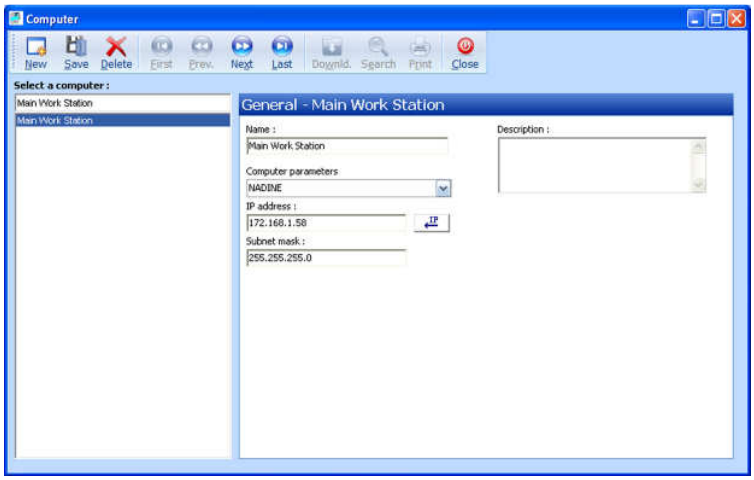
Define the computer/s on which the application will run and all supported workstations.

The first time the application runs, the fields **Name**, **Computer Parameters**, **IP Address** and **Subnet mask** will be filled automatically, taking the parameters of the machine on which the application is running.

If for some reason the computer is replaced, then in addition to restoring the database on the new PC, the application will request that the operator updates this screen with the new IP address.

Subsequently, this screen is used for defining additional workstations.

Click **New** to start definition of a new workstation.



Name: Free Text

Computer Parameters: Lists of all computers on the network – select the computer to be used as a workstation

IP address: Clicking the IP arrow will automatically update this field for the selected computer

Subnet mask:

New installations: The application can use multicast addressing, and the application uses an **alias** Subnet Mask setting of 239.0.0.60 (multicast address) to enable this. Therefore the application sets this mask as a default in the screen. No change should be made to the Windows settings.

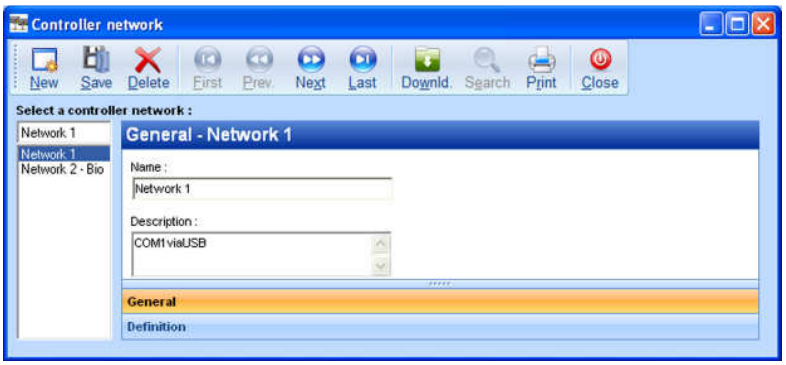
Fields only show after pressing Shift+F12

Restart and Shutdown: These will be invoked automatically within 2 minutes of pressing the button. A warning message is presented before the instruction is activated.

3.2 CONTROLLER NETWORK

3.2.1 CONTROLLER NETWORK / GENERAL

"Network" refers to the physical/electrical connection by which controllers are connected to a PC. This screen allows a Network to be named, and once this is done, the following Controller Network/Definition screens allows input of the required configuration details, depending on the type of Network being defined: local, TCP or modem comms port.



Name: Free text. Default name is <Network1> – can be edited

Description: Free text

Notes:

Configuring Bio Reader Network Bio Readers are connected to regular controllers but also require their own dedicated network for transfer of Bio template data to and from the computer. Separate network/s must be defined for this purpose.

Pressing Shift+F12 allows displays Advanced Network Settings used when setting up a 2nd communications bus for the controller. 3.2.1 Controller Network/Definition

3.2.2 CONTROLLER NETWORK / DEFINITION

There are three connection methods supported: local communication port, IP network, and remote (modem). This screen allows the definition of networks of each of these types.

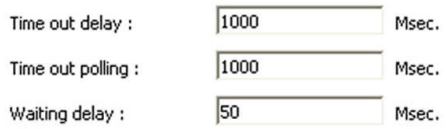
Select a Controller Network: Click New to define a new network

Port: Select the required connection method. When this selection is made, the additional fields necessary for the selected type of network are displayed.

Encryption Key: When checked, a 4-digit Hexadecimal (i.e. 32-bit) Encryption Key may be entered (Min. value: 01 00 00 00 / Max value: 7F FF FF FF)

This key secures the data traffic between the PC and the controllers by encoding the information that passes over the communication bus (whether serial or TCP/IP). Each controller network may have its own key. When the PC and the controllers communicate, each data packet is encrypted using this password, preventing a hacker that has a copy of application software from accessing the controllers.

Communication Parameters



For any type of Controller Network, the following Communication Parameters must be defined.

Caution: Defaults of these parameters should only be changed by experienced Communications engineers.

Time out delay (Default 1000 msec – keep this value unless specified otherwise), Delay in millisecs

The timeout delay is the maximum time within which a controller must answer to a command sent by the system. If the controller does not answer within this time, the system will try n more times (default 2) to send the command (value set in Tools/Options/Communication).

If there is still no answer from the controller, the command will be put in the Pending commands.

Time out polling (Default 1000 msec - keep this value unless specified otherwise), Timeout in millisecs

Polling a controller means asking it if any events just occurred, i.e. either a card transaction (granted or denied) or an alarm. In polling mode, the system continuously polls all controllers, and they must answer either with an empty message, if nothing happened, or with the last event(s) that occurred. The ‘Time out polling’ is the maximum delay, measured in milliseconds, beyond which a controller must answer a poll. If the controller does not answer within this delay, the system will try n more times (default 2) to poll it. (value set in Tools/Options/Communication).

If there is still no answer from the controller, it will flag this as a communication error and jump to the next controller.

The system will declare a communication problem if a controller does not answer to polling during a pre-defined ‘Polling error time-out' delay.

The ‘polling error time-out' delay (30 seconds by default) is adjustable in Tools/Options/Communication

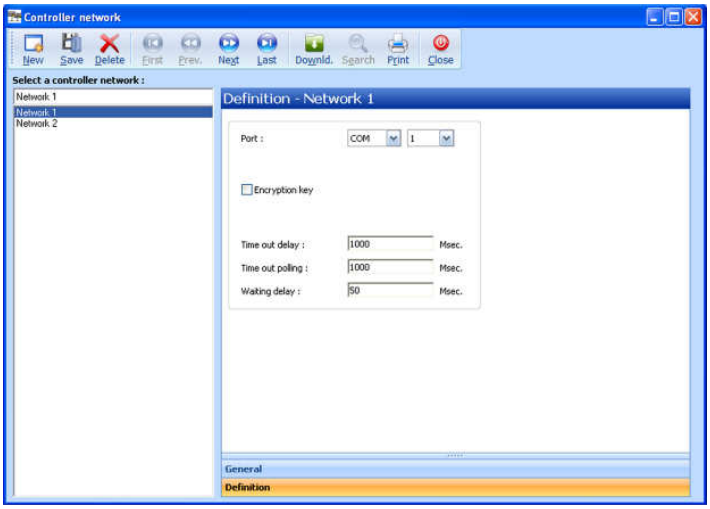
Waiting delay (in milliseconds)

(Default 500 msec – keep this value unless specified otherwise)

Specifies the delay between two communication operations between the system and the controllers (polling or commands) - measured in milliseconds. This function will help slow down the system so as to free up the system PC.

Note on Baud Rate: The communication baud rate between controllers and the system is defined in Tools/Options/Communication

3.2.2.1 LOCAL COMMS PORT



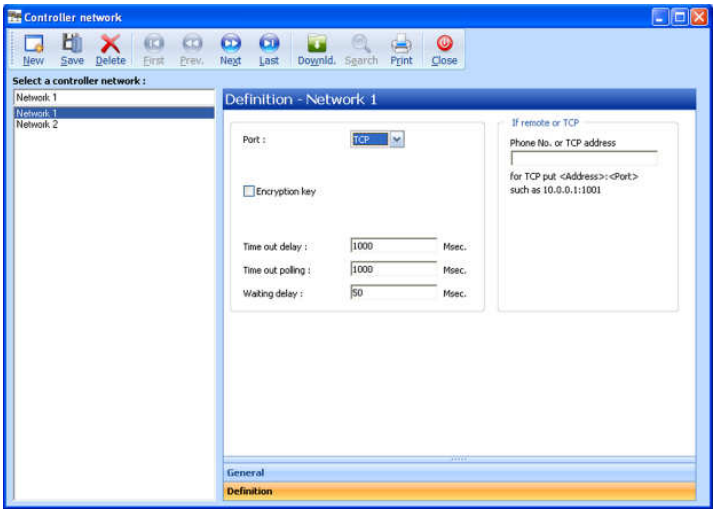
This screen defines a Communications Network connected via a PC Port (COM 1, . . .n).

In the screen example, the pull-down shows the Network type as 'COM'.

Port: Select 'COM' and choose a COM port number, from 01 to 99

PC Port per COM Network
Each network defined as type 'COM' must have a separate corresponding port on the PC.

3.2.2.2 TCP COMMS PORT



This screen defines a Communications Network connected via a TCP network.

Port: Select 'TCP'

Phone no. or TCP address: Specify the TCP address requested in the format '<Address>:<Port>'. Example: 192.168.168.49:1001

3.2.2.3 MODEM COMMS PORT

This screen defines a Communications Network connected via Modem.

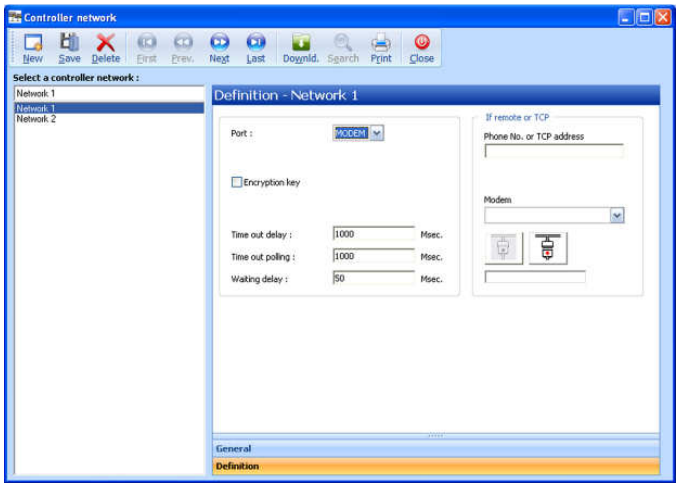
Port: Select ‘Modem’

If Remote or TCP

Phone No. or TCP address: Enter the Phone number that the remote modem will be using

Modem: Pull-down to select a modem: (the list corresponds to the modem drivers installed on the PC)

- Set modem to auto-answer
- Configure modem to match Controller settings
- Click Connect button
- See Updating Remote Controllers for further info



Connect/Disconnect buttons:

Note: These icons are enabled only after the definition of a new network controller has been saved

Connect button - Initiates the modem connect sequence.
The status will be shown - (‘Proceeding’, ‘Line Busy’, ‘Connected’)

Disconnect button - Takes the controller off-line. Relevant database changes will be saved until the next time the controller is connected.

Notes:

1. Default values for communication parameters are set in *Tools/Options/Communications*.
2. See notes below for Updating Remote Controllers.

3.2.3 UPDATING REMOTE (DIAL-UP) CONTROLLERS VIA THE MODEM

When remote controllers are connected to the PC through a communication port defined as ‘Modem’ (in the ‘port’ field of the Controller Network/Definition Tab), and the user makes changes to the database, dial-up Controllers can be updated in three ways:

Update Controllers Manually

Open the definition in Controller Network and click ‘Connect’. Once the controller is online, all the ‘pending’ commands are downloaded automatically, and all events stored in the controller are uploaded.

Update Controllers by User-defined schedule

Modem dial-up may be automatically performed within predefined schedules. Refer to the complete User Manual for details.

Update Controllers by Automatic Dial-up

When a local controller does not answer to controller commands, (usually due to a communication problem), these commands are left as pendings in the buffer of the controller, and are cleared as soon as communication is restored.

For remote controllers, the system can automatically connect to update pendings on a regular basis. Refer to the complete User Manual for details.

3.3 CONTROLLER

A controller is a microprocessor-based electronic circuit board with a large onboard memory for storing the various parameters to be monitored, such as cardholders, time zones, reflexes, etc. Controllers are connected to the central system via dedicated Networks and the onboard parameters for each controller are downloaded to them from the central system.

A controller supervises the following components of the security system:

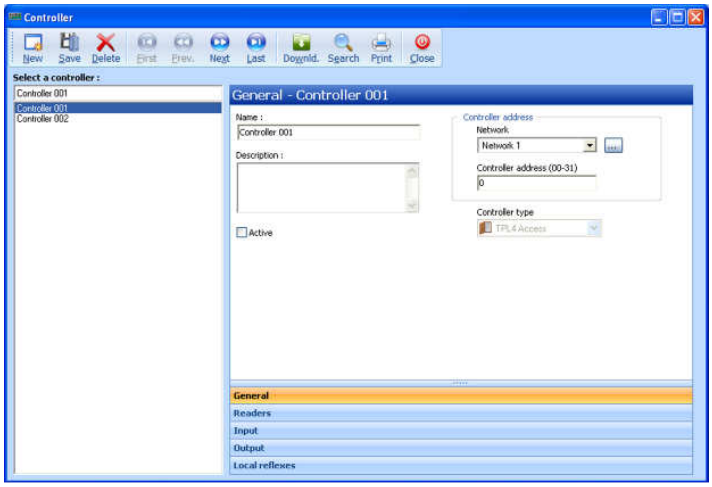
- **Readers** (and their corresponding doors): Various types of readers may be supported, although installations normally only have one type. Where more than one type needs to be supported, these may not be mixed on a particular controller.
- **Inputs:** Controllers have banks of inputs, i.e. electrical connection points that may be connected to external sensors/detectors to sense external events (Door contacts, Door remote control (called ‘Request-to-Exit’ or ‘RTX’), Motion detectors, Passive infra-red, etc). These are usually used for alarm management.
- **Outputs** (Relays): Controllers have multiple Outputs that can activate external devices. (door locks, audible signals, indicator lights, etc.)

Readers, Inputs and Outputs are user programmable from the Controller screen.

These menu and sub-menu screens allow definition of the controller's parameters in the system.

3.3.1 CONTROLLER / GENERAL

This screen allows definition of the controller's parameters in the system.



Name: <Controller 001>, <Controller 002>, . . are default names and these may be modified by the user.

Useful Note: Use of logical names allows the user to recognize which controller is referred to. (e.g. 'FrontEntrance01', 'FrontEntrance02' etc.)

Description: Free text

Active: Check to activate communication. Uncheck to set offline.

Same Definition as: This dropdown appears only when **New** is pressed. It allows a new Controller to be defined using the same settings and parameters as a currently-defined controller.

Network: Select an existing network from a list of previously defined networks or create a new network by clicking on the […] button.

Controller Address (00-31): Enter the physical address of the controller as set on the controller Address Selection DIP switches.

Controller Type: Select correct type from the list of *Controller Types*.

Parking: (displayed only if the selected Controller Type includes the description 'Parking') Use dropdown to select the Parking Lot to be associated with this Controller.

Notes:

1. **Saving and downloading:** When saving the data entered (Save or F3), automatically downloads any relevant data from the new information entered. If the controller has just been created, a complete download will be performed, which includes: initialization data, update of time and transfer group parameters, daily and weekly programmes for access, reader parameters, card format and cardholders database (with access authorizations).

2. **Updating:** Once a controller type has been selected and the entry saved, the controller type may not be changed. To change the type, you must delete the controller and make a new one.

3. **TPL4 Lift & TPL4 D4 Lift:** A single controller can pilot several lifts independently.

3.3.2 CONTROLLER / READERS

These menu and sub-menu screens allow definition of the Reader's parameters in the system.

READER LIST

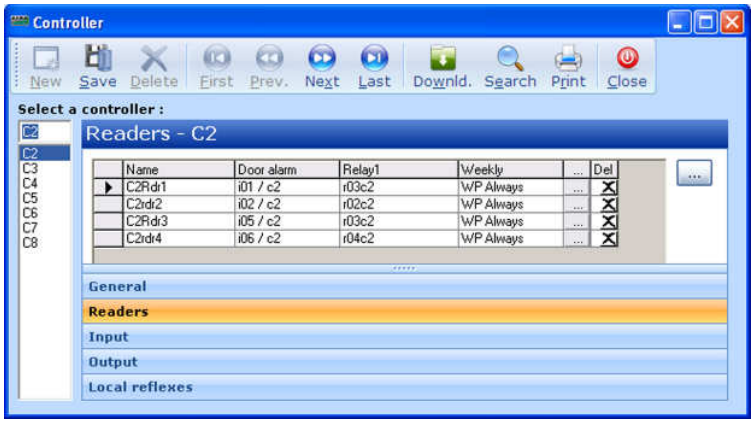
Selecting the Reader Tab displays a List window, from which a reader can be selected.

The List window shows all readers defined for the selected controller. Default parameters are defined according to the type of controller.

Click on the **[...]** symbol of the required reader in this screen to open the General tab screen for that reader.

Reader Tab: Readers - <Controller n>

A table of all the readers of the selected Controller is displayed, showing Reader name, Door alarm (the alarm that signals opening of this door), Relay1 name, and the assigned weekly programme



➢ **:** Use Up and down arrows to select a Reader

[...]: Click to open the *Readers/General* screen for the selected reader: Click to delete the selected Reader

✖ **:** Click to delete the selected Reader

[...]: (Outside the list table) – Click here to access the *Readers/General* screen returning to the top of the list.

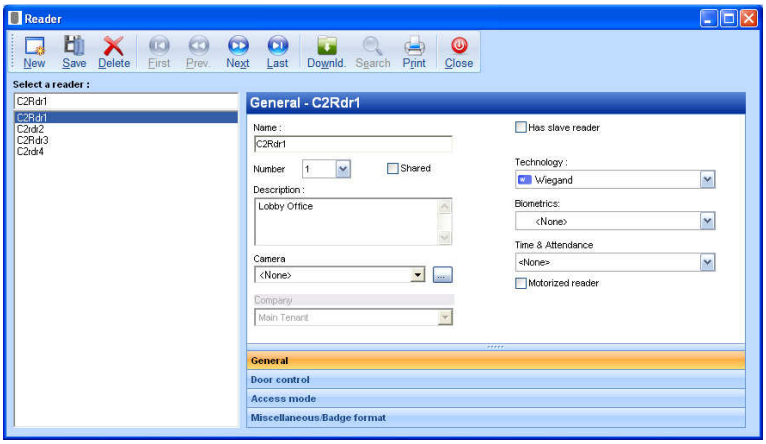
Note: If an alarm controller (such as 'DS200' or 'TPL4 Alarm') is selected, the system displays the message: "Alarm monitoring controller without readers!"

3.3.2.1 READERS / GENERAL

This screen allows the user to assign a name and description to the selected reader and define basic characteristics.

Name: Reader name – free text

Useful Note: Use of logical names allows the user to recognize which reader is referred to. e.g., 'Front Entrance Main Street', 'Main Entrance Production hall', etc**.** The abbreviation 'Rdr' is used in default names to show the difference between Readers and Relays (Rdr01, Rdr02 . ., rather than r01, r02 . .)



Number: Dropdown shows available readers defined for that controller

Description: Free text

Camera: (only for use with Video Module) Select Camera from list if associated with this door. If not defined yet, click [...] to open Camera screen

Has Slave Reader: If the controller is a "Two-door controller', only two doors may be controlled. However, by checking this box, a second ('slave') reader can be added to each door, to control movement in the opposite direction. This slave reader doesn't have its own parameter screen - it has exactly the same parameters as the main reader.

Technology: Default technology as selected in *Tools/Options/General* screen will be shown. Dropdown can be used to select a different technology.

> **Caution**: If the technology specified for a reader (in the screen) is changed, the system will automatically change ALL other readers on the same controller to the new technology. The database of cards on that controller will be deleted and a new database holding only cardholders with the new technology will be downloaded. Care should be taken before making such a change as this can result in the downloading of a large number of records, creating a substantial load on the network to which the controller is attached.

Biometrics: If a Biometric technology reader is selected, choose the required biometric from the dropdown. The Fingerprint Tab is only displayed if the selected reader has biometric capability

Time and Attendance: According to the T&A variation in use, select as follows:

Standard T&A option 1 -

Select **'none'**. (The 'Standard T&A Option 1' system report uses only the first and the last transaction of the day, from any reader)

Standard T&A option 2 –

Select **'Entrance reader'** if working time calculation will start from this reader
Select **'Exit Reader'** if working time calculation will stop at this reader.

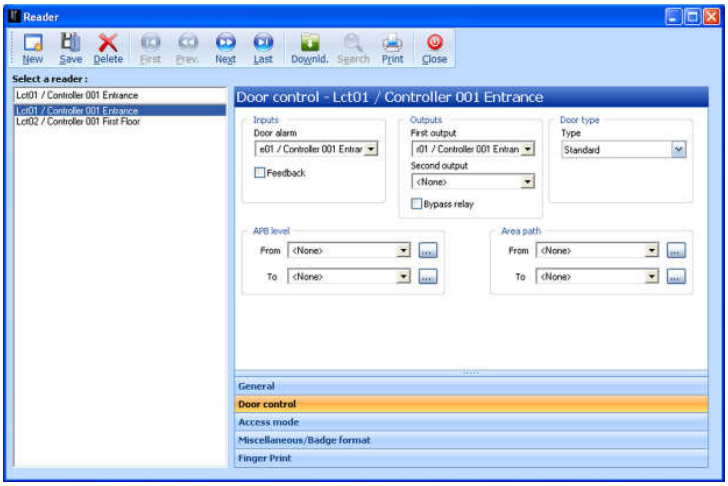
T+ Module - Select **'Entrance Reader/Exit Reader'** if the reader is to be used for reporting T&A transactions.

Motorized reader: Check box if motorized reader attached. To use the DDS magnetic motorized readers, select the 'Motorized Reader' technology in this screen. Two additional fields are displayed:

Select the controller input connected to the badge detection signal (S1)
Select the controller relay to which the Common is connected to the signal (MFC/MRC) that controls the sense of the reader motor.

3.3.2.2 READERS DOOR CONTROL TAB

This screen defines which Controller Inputs and Outputs are used for door sensors, controls, and alarms, defines the type of doors installed and specifies the APB levels and Area before and after a badge is passed at the Reader.



Inputs

Door Alarm: Select the controller input to which the door opening control device ('door contacts') is wired; an alarm is set off when a door is forced or stays open beyond a predefined delay ('door alarm delay') – see Reader/Access Mode screen

Feedback: Check the box in order to verify the physical entry or exit of a cardholder that has been granted access (i.e. that after reading a badge and granting access, that the door actually opened)

Operation mode**:** A cardholder swipes a badge at a reader. The controller authorizes access to the cardholder by activating a door relay. During the predefined 'door open' time, during which the door can be opened, the controller goes into a waiting mode.

If the door has been opened and closed, as sensed by activation of the ‘door opening control device’, the cardholder is assumed to have passed and the controller records the access transaction in memory.

If the door is not opened, the ‘door opening control device’ is not activated and the controller records the transaction “access refused – door locked” in memory.

Outputs: Two relays (‘first and second outputs’) may be activated when access is granted to open doors, gates, etc. Select them from the list of relays defined on this controller. They are activated during the ‘Door open time’ delay. - See *Reader/Access mode* screen

Bypass relay: When this check box is selected, then when access is granted, the second relay is activated for the duration of the 'Door alarm delay' and not for the ‘Door open time’ – (See *Reader/Access mode* screen). It is automatically deactivated when the door is closed.
Typically used where an authorized employee must enter to switch off an alarm panel, etc. A ‘bypass’ relay is connected to inhibit the Door Alarm input of the Alarm Panel during the programmed door alarm delay. (Requires firmware dated 16/03/09 and later).

Door type: Select from list:

Standard: Access is granted if badge is authorized

Controlled by Input: This specifies that the door is controlled by the status of the input specified in the ‘Controlled by’ field. The door opens if that input is inactive but remains closed if it is active. (If, for example, the input selected is the door contact of a second door, the ‘controlled’ door will be opened only if this second door is closed)

Man Trap 1, 3, 4: Select if the doors operate in man trap mode, i.e. passage through two consecutive doors is required in order to access a site.

Manually Controlled: Access is manually regulated

APB Level: Anti-Passback levels divide the site into ‘levels’ which are geographic zones delimited by readers. The system may control the movement of people so that they have to follow a specific path, i.e. pass between specific levels in a defined way

From: Select the APB level where the cardholder who requests the access must be, or <none>, from dropdown. Use [...] to define a new APB level

To: Select the APB level that describes where the cardholder will be after passing a badge at this reader or <none> from dropdown. Use [...] to define a new APB level

Area Path: Area Paths divide the site into ‘areas’ and allow the system to determine the number of people currently inside a named ‘area’ – Areas can be

defined for the whole site, building/s (or floor/s of a building), and/or a particular room or rooms.

From: Select the Area that describes the area that the reader is in or <none> from dropdown. Use [...] to define a new Area

To: Select the Area that describes the Area where the cardholder will be after passing a badge at this reader

3.3.2.3 READERS ACCESS MODE TAB

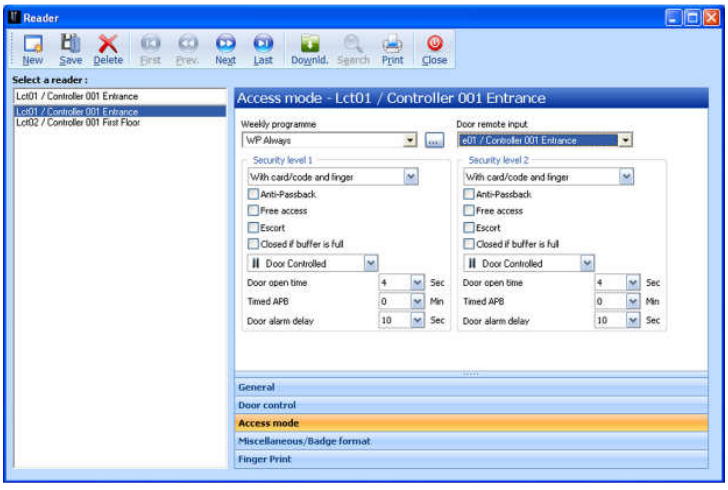
Every reader has two sets of settings – 'Security level 1' and 'Security level 2', allowing different access controls to be applied when reading a badge.

The current Daily Programme for each reader (set up in the Weekly Programme associated with it) divides the day into 2 segments:

'Time Zone 1' - (**green** time) – during this time, the reader uses the rules of 'Security level 1'

'Time Zone 2' - (**red** time) – during this time, the reader uses the rules of 'Security level 2'

Note: Maximum number of usable programmes
Many daily, weekly and holiday programmes can be created in the whole system. However, **each controller** may only include a restricted number of programmes. An error message appears if the limit of programmes has been exceeded for a specific controller.



Weekly Programme: Use the dropdown to select a Weekly Programme for the reader, or the [...] field to create a new *Weekly programme* or modify an existing one.

The reader automatically selects its current 'Security Level' based on the Time Zone set in the Weekly Programme associated with it.

The default Weekly Programme for all readers is 'WP Always' and therefore a reader will operate in 'Security level 1' unless another Weekly Programme is selected.

Door remote input: Select the controller input to which the Request to Exit button (RTX) is connected.

Note that when an RTX input is associated with an Event Weekly Programme (via the 'Event Handling Programme/Alarms' screen), the button is active and raises an alarm during the 'green' periods of the Weekly Programme but doesn't open the door (and doesn't raise an alarm) during the 'red' periods of the programme.

Security Levels 1 & 2:

Define the access rules applicable to the two states of the Weekly Programme.

These parameters must be filled out separately for **both** Security Levels 1 & 2

Security level 1 – Green time**:**

Rules to apply during Time Zone 1 of the applicable Daily programme

Security level 2 – **Red time**:

Rules to apply during Time Zone 2 of the applicable Daily programme

Parameters for Security Level 1 & 2

Access authorization: Define the way in which the authorization access must be initiated:

With Card (normal card read)

With Keypad (just enter PIN at Keypad (Personal Identification Number)

With Card OR Keypad

With Card AND Keypad

Note: If the .ini entry *DisplayandSaveOnlyGrantWithPIN*=1 is set, the Application will **only** show and save Grant events where **both** badge and PIN were used to grant access.

Anti-Passback: Check this box if APB is to be applied at this reader. The Anti-Passback feature is used to stop a card from being used for successive entries without a valid exit, or vice-versa.

Free Access: Check to set this reader to provide unlimited access for any valid cardholder without checking their validation date or their access group.

Example: This setting could be used when all employees must be temporarily allowed access at this reader, such as access to a normally-restricted area for a Company event...

Escort: Checking this box requires that anyone passing their card at this reader have their transaction validated by a second cardholder. The second badge must be presented within the time set in the 'Door open time' parameter (4 secs default). (The second cardholder is noted in the log as having accompanied the first, but does NOT get their own transaction).

Note: If 'escort' is checked, then the 'escort' (i.e. the second card read) may normally be any cardholder. However, if the Cardholder requesting access has the

field ‘Need escort’ checked in his Cardholder/personal screen, then the second cardholder must be registered as a ‘Supervisor’ in his Cardholder/Personal screen, in order to act as their escort.

Close if buffer is full: Select this function to refuse access when the corresponding transaction cannot be registered in the system Event Buffer, because it is full. It must then be read form the PC and erased to allow accesses.

If this option is not selected, access is granted even if the buffer is full. The buffer then operates as a ‘FIFO’ buffer, i.e. the oldest transactions are erased in order to make space for the newer ones.

Door status: A door can be set to three different states:

Door controlled – Standard access mode, access depends on badge and authorizations

Door closed – door is closed and no access permitted while in this state, regardless of badge and authorizations

Door open – door is open, access control not in force

Door open time: (0-120 secs) Time during which cardholder may pass through after receiving authorization. This corresponds to activation delay of the relays that control the door.

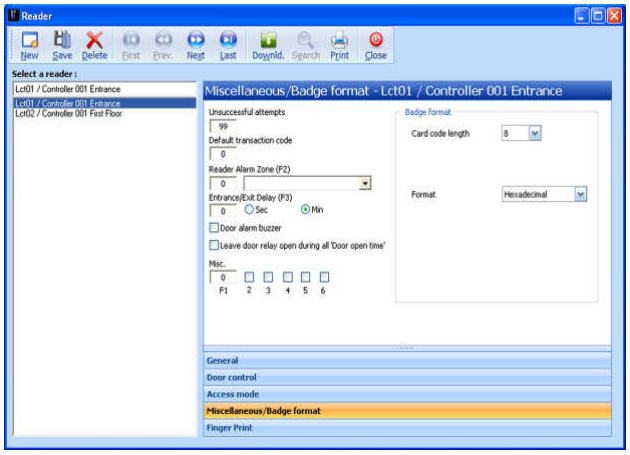
Note – Alternated Mode – By setting the time to 122 secs, the door will be set to a mode where it will stay open after a valid badge is read and only close when a second valid badge reading is completed and so on.

Time APB: Delay before the same person can use the door for a second time.

Door alarm delay: (0-75 secs, to nearest 5 secs) - Delay during which the door must be closed. If the door is still open after this delay, a ‘Door left open’ alarm is raised.

3.3.2.4 READERS MISCELLANEOUS/BADGE FORMAT TAB

This screen allows the user to define a number of additional parameters for the reader.



Unsuccessful attempts: Specify the number of successive unsuccessful attempts allowed by the system before an alarm is raised (00-99)

Default Transaction code: Specify the transaction code sent by the

controller to the PC when an access is granted. If the reader is equipped with a keypad, the user can modify this default code.

Transaction codes are used for the following functions:

- o T+module T&A transactions: The system will associate a Work Category with the Transaction code
- o Pre-defined action(s) may be triggered by the system upon reception of specific transaction codes.
- o Readers with special Supervisor functions

Reader Alarm Zone (F2):

This field may have two functions:

- o **Associate an Alarm Zone** (also called 'Input Group') with the reader: When a Reader Alarm Zone is selected in this field, then access through the reader is denied when the selected Alarm Zone is armed, excepting for supervisors: the zone is then temporally disarmed during the 'Entrance/Exit delay' to allow the supervisor to access the zone and disarm it from an indoor alarm panel.
- o **Define a specific code for a keypad function key:** For readers equipped with a keypad and function keys F1/F2/F3, this field may be used to define a code which is sent when access is granted and the [F2] function key is used. In that case, the controller which manages this keypad reader may not control Alarm zones.

Entrance/Exit delay (F3):

This field may have two alternative functions:

- o **Alarm zone disarm/armed delay:**
  - If the reader controls the entrance zone, this field defines the entrance delay, in seconds or minutes, during which the reader alarm zone is disarmed when a supervisor is granted access via this reader.

  - If the reader controls the exit zone and is equipped with a keypad, this field defines the exit delay, in seconds or minutes, during which the reader alarm zone stays disarmed when a supervisor armed the zone from the keypad (using command 26zz where zz is the zone number). After the delay, the zone is armed.
- o **Define a specific code for a keypad function key:** For readers equipped with a keypad and function keys F1/F2/F3, this field may be used to define a code which is sent when access is granted and the [F3] function key is used. In that case, the controller which manages this keypad reader may not control Alarm zones.

Door alarm buzzer: Check this box if the reader buzzer is to be activated if the door either opened without authorization or if it remains open too long after a valid pass.

Leave door relay open during all 'Door open time': In the Default setting (i.e. when this box is NOT checked), the controller deactivates the door relay as soon as

it detects that the door has been opened (through the door sensor). Checking this option will leave the relay activated during the 'Door open time'.

Check connection*: To enable automatic report transaction if reader disconnected. (* Only supported on Mega and TPL-DR controllers)

3.3.3 CONTROLLER / INPUT

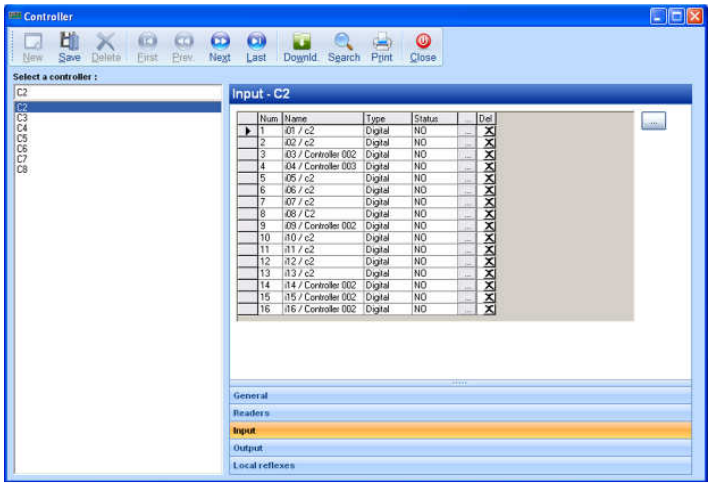
A Digital Input or Alarm Input is a controller input point to which a sensor/detector is connected (examples - magnetic contacts, movement detectors, door contact device to reflect the door position, etc…). In general, controllers have by default 4 or 8 inputs and may be extended to 16 or more. The two input status open or closed correspond to the two possible physical status of such sensor/detector: open or closed.

When armed, inputs may raise an alarm either immediately when activated (i.e. when their status changes from 'alarm-off' to 'alarm-on') or after a pre-defined delay. Inputs can be grouped together into 'Inputs Groups' also called 'Alarm Zones'.

From the *Controller/General* screen, selecting the Input Tab displays a List window, from which an input can be selected.

The informative table summarizes the parameters of the controller's Inputs. Default parameters are defined according to the controller type.

Click on the […] symbol of the required input to open the Controller/Input/General *screen*.



Input Tab

Input - <Controller n>: A table of active inputs for that Controller is displayed, showing Input name, Type, and Status

➢ **:** Move the indicator up and down with the cursor arrows to select an Input

[...] (on a specific Input entry): Click to open the *Controller/Input* screen to define the selected Input

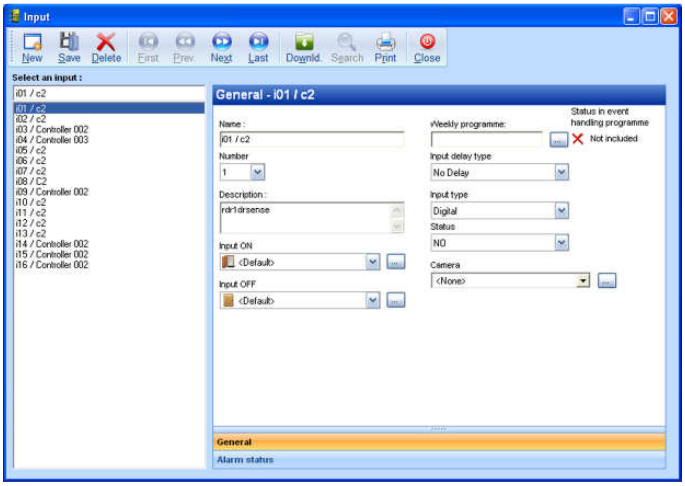
✖ **:** Click to delete the selected Input

[...] (outside the list table): Click here to access the *Controller/Input* screen to define a new Input (i.e. without selecting an existing Input)

3.3.3.1 CONTROLLER / INPUT GENERAL

The Input screen allows definition of the Input parameters.

Note for sites using Alarm Monitoring module: Many of the Alarm Monitoring features are activated by 'Alarm zones (also called Input Groups)' rather than individual Inputs. For that reason, it is recommended that sites using the Alarm Monitoring module should use Input Group definitions for inputs, rather than use defining individual Inputs



Name: Free text

Number: Select Input Number from dropdown, according to Controller Type

Description: Free text

Input ON: Use dropdown to select Icon to be displayed on the maps when this input is in the alarm_ON condition.

Clicking [...] opens the *Controller/Outputs/Icons Tab* screen, allowing a new Icon to be added to the list

Input OFF: Use dropdown to select Icon to be displayed on the maps when this input is in its normal state (NOT **alarm_ ON**)

Clicking [...] opens the *Controller/Outputs/Icons Tab* screen, allowing a new Icon to be added to the list

Camera: Use dropdown to select Camera to associate with this Input. Click [...] to create a new Camera definition. Note: Only for use with the Video module

Weekly programme: A Weekly Programme defines alarm arming or disarming periods. This is a display-only field which shows to which Weekly Programme the alarm is assigned. To choose a different Weekly Programme or to assign one if not yet assigned, click on […] to open the *Event Handling* screen.

Status in event handling programme: Shows whether this Input is Included (✓) or Not Included (×) in this Weekly Programme.

Note: This indicates only the status of the input as an individual. It may be armed/disarmed as a member of an Input Group (Alarm Zone), but that will NOT be indicated on this screen. To check if that is the case, check the Input's status using the *Active Alarms/Input* screen.

Input delay type: Select type of delay

- **No delay**: An alarm is raised as soon as the input is activated
- **After… (if on alarm)**: Alarm will be raised after … seconds, only if Input is still activated
- **After… (even if no more on alarm)**: Alarm will be raised after … seconds, even if Input is no longer activated

Input type: Select Input type:

- **Digital:** open or closed, i.e. the two possible states of the sensor/detector connected to the input
- **Digital (4 states) (also called 'supervised'**): in addition to two states above, the input may detect the states Line_cut or Line_short corresponding to the status of the line that connects the sensor/detector to the input

  Note: A2-state input **may not** be defined as 4-state, but a 4-states input **may** be defined as 2-state provided that the line does not need to be supervised.

Consult the controller documentation to check which types of inputs are available on the controller.

Status: Select the status -

- **NO - normally open:** the input will raise an alarm if, while it is armed, its status changes from 'open' to 'closed'
- **NC - normally closed:** the input will raise an alarm if, while it is armed, its status passes from 'closed' to 'open'

3.3.4 CONTROLLER / OUTPUT

Controller **Outputs** refer to the output contacts of a controller relay. In general, controllers have 4 relays (by default – this may be extended to 16 or more). Such relays provide a 'dry contact', and may be regarded as an electrical switch which can be either open or closed. When the relay is closed, the device (door, siren, etc.) which is connected to the relay is activated, assuming that it is powered-on.

The output state is the state of the relay, i.e. closed (or activated or 'on') or open (or deactivated or 'off').

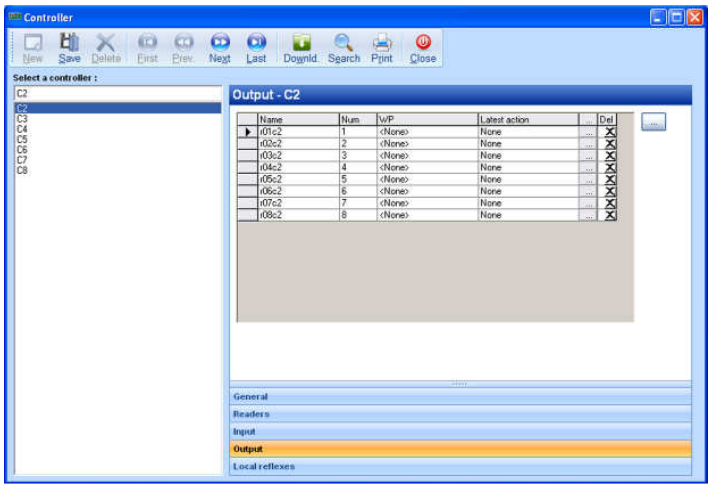
An Output is opened upon specific events as follows:

- Access granted (in the case of an Output which controls a door opener)
- During time period defined by a Weekly Programme associated with the Output
- According the status of the Alarm Zone (armed or disarmed) associated with the Output.
- By pre-defined automation steps (Reflexes, etc.)
- By manually invoking a Process (one or more Actions).

From the *Controller/General* screen, selecting the Output Tab displays a List window, from which an Output can be selected.

The informative table summarizes the parameters of the controller's Outputs. Outputs are the relays on the controller board (or on its extension board) to which external devices may be connected and activated by the controller - Door openers, sirens, etc.). Default relays numbers are defined according to controller definition.

Click on the […] symbol of the required Output in this screen to open the *Controller/Output/General* screen.



Output Tab

Output - <Controller n>: A table of active outputs for that Controller is displayed, showing Output name, Number, Weekly Programme,

➢ **:** Move the indicator up and down with the cursor arrows to select an Output

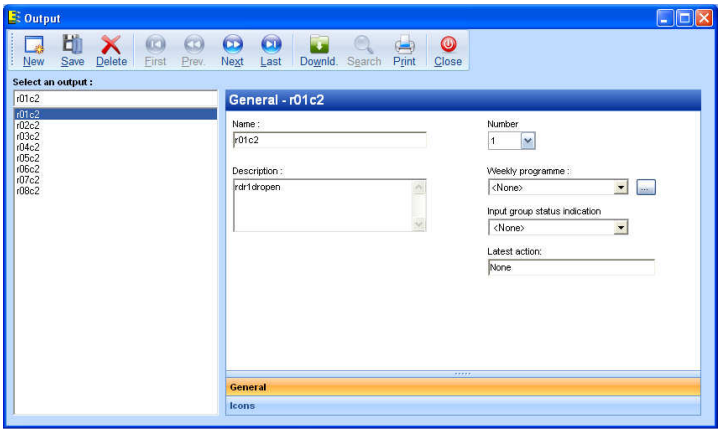
[...]: Click to open the Output Tab screen to define the selected Output

✖ **:** Click to delete the selected Output

[...]: (Outside the list table) Click here to access the *Output Tab* screen to define a new Output (i.e. without selecting an existing Output)

3.3.4.1 CONTROLLER / OUTPUT GENERAL

This screen defines parameters for Outputs.



Name: Free text, Default name is <Reader n/ Controller n>

Description: Free text

Number: Select from dropdown. Maximum number of Outputs depends on Controller Type

Weekly programme: When a Weekly programme is selected, the relays will be automatically activated during the 'green periods' defined by this programme (and deactivated during the 'red periods' of the programme).
Click on […] to create or modify the weekly programme.

Caution **-** Do not allocate weekly programmes to Door Relays. Time activation of door relays must be set from the *Reader/Door control tab*. Allocating weekly programme through this *Controller/Output* screen may result in a definition conflict.

Input group status indication: By selecting an Input Group (Alarm zone) from this dropdown, the Output will be assigned to act as an Input Group status indicator: when the Input Group (alarm zone) is armed/disarmed, the relay is automatically on/off

(Requires DS216 firmware from 24.06.09 or later and TPL firmware dated 23.05.09 or later).

Latest action: Displays the last Action that affected the Output - this can be caused by either of the following:

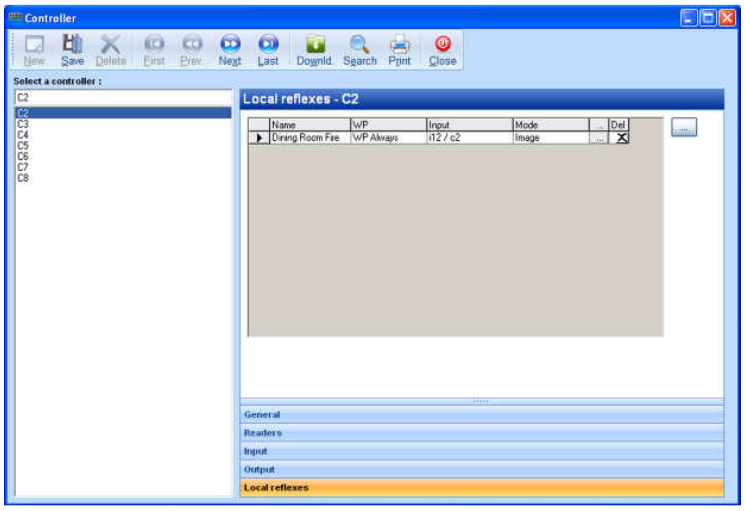
- a **Manual Action** (see Action button in *Manual Actions/Relays Control* screen – Only Constant_On and Constant_Off commands are shown)
- an **Action/Process** activated manually or activated by a Global Reflex or other reasons that would trigger a Process automatically, such as Guard Tour, Counter, Parking.

3.3.5 CONTROLLER / LOCAL REFLEXES

A local reflex defines the output activation following the trigger of an input of this same controller.

From the Controller/General screen, selecting the Local Reflexes Tab displays a List window, from which a Local reflex can be selected.

The list summarizes the parameters of the local reflexes associated to the controller, and clicking on the […] symbol opens the *Local Reflex/General* tab.



Local Reflexes Tab

Local Reflexes - <Controller n>: A table of local reflexes for

that Controller is displayed, showing local reflex name, Weekly Programme, Input and Mode

➢ **:** Move the indicator up and down with the cursor arrows to select a Local Reflex

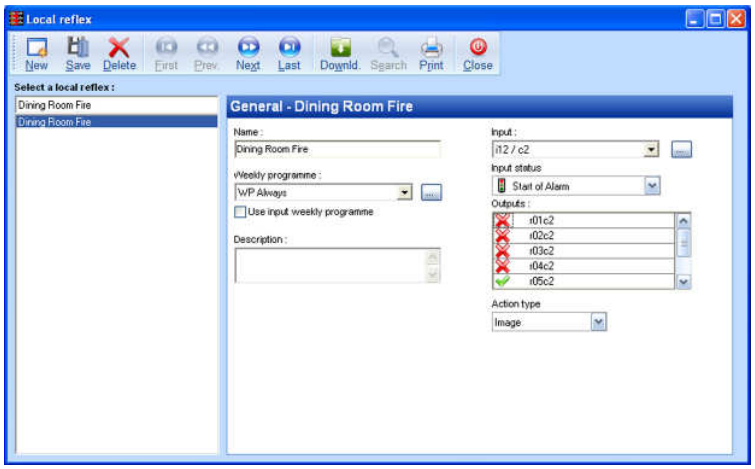
[...]: Click to open the *Local Reflexes Tab* screen to define the selected Local Reflex

× **:** Click to delete the selected Local Reflex

[...] (Outside the list table): Click here to access the *Local Reflexes Tab* screen to define a new Local Reflex (i.e. without selecting an existing Local Reflex)

3.3.6.1 CONTROLLER / LOCAL REFLEXES GENERAL

A Local Reflex defines the Output activation following the trigger of an Input on the same controller. Note that because the Inputs and Outputs are on the same controller, the reflex is managed by the controller and occurs even if communication with the controller is interrupted.



Name: Free text

Weekly Programme: Use dropdown to associate this Local reflex with a particular Weekly Programme.

Note: The Local Reflex will be activated during 'green' times in the Weekly Programme selected.

Click [...] to create a new weekly programme

Use input weekly programme: If checked, the Weekly programme associated with the reflex is the one defined for the Input itself. If this is done, then this disables the option (above) of associating the Local Reflex with its own Weekly Programme.

Description: Free text

Input: Use dropdown to select the input triggering the local reflex. Click […] to create a new input

Input status: Select the status of the input which sets off the local reflex: Start of alarm, End of alarm, Line cut, Line short, Open, Close, <Any Status>**.**

Outputs: Click on the ✓ or × buttons, to set which relays to activate

Action Type: Choose the type of action set off by the local reflex:

- **Image**: When the input is activated, the relay(s) is/are activated. When the input is deactivated, the relay(s) is/are deactivated at the same time
- **Constant ON**: When the input is activated, the relay(s) is/are activated and stays activated, even if the input is deactivated. The relay(s) must be deactivated by manual actions.
- **During**: When the input is activated, the relay(s) is/are activated for the predefined **Duration Time** (1 – 120 sec., 122sec for 'Alternated')

Note: When this parameter is set to 122 sec, this defines **'Alternated mode'**: The relay(s) is/are activated after the input is activated and stay/s activated; the relay(s) is/are only deactivated after a second input activation and stay/s deactivated, and so on.

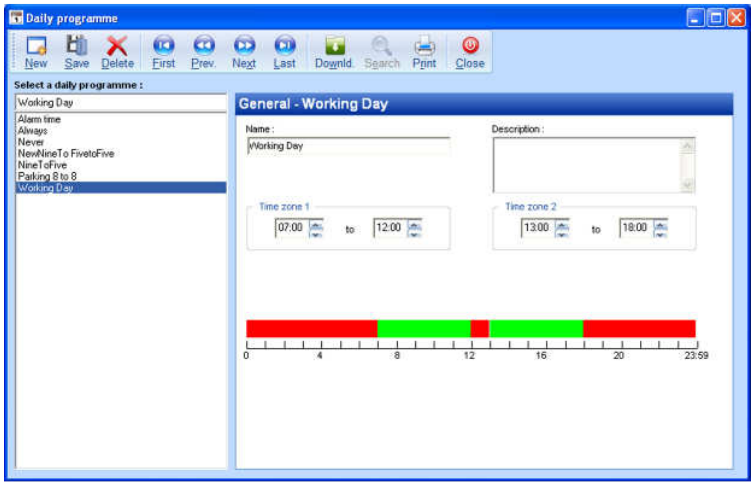
3.4 TIME ZONE

Weekly Programmes (which are made up of Daily Programmes with their associated Time Zones) are an important concept in the system. As any event occurs (e.g. a badge is passed at a particular reader, an Input status changes, etc), the system compares the actual time against the Daily Programme associated with that event, and acts in accordance with the rules set for the current Time Zone in that Daily Programme.

3.4.1 DAILY PROGRAMME

A regular Daily Programme divides a 24H day into segments defined as 2 (or 4) **Time Zones**. With 2 Time Zones, there will be 2 '**green**' time periods (the Time Zones), and 3 '**red**' periods.

Where a more complex day is required, it is possible to divide each day into 4 times zones and therefore create 4 'green' periods and 5 'red' periods (by changing the option '2 time zones' to '4 time zones' in the field 'Daily Programme Time zones' – see Tools/Options/Communication)



Name: Free text

Description: Free text

Time Zone 1: Start and end times of 1st 'Green' time zone

Time Zone 2: Start and end times of 2nd ‘Green’ time zone

Ruler: The ruler displays the Green and Red times visually

Notes: The system maintains two default daily programmes – ‘Always’ and ‘Never’. The names of these programmes can be edited, but they cannot be deleted, nor their parameters modified.

3.4.2 WEEKLY PROGRAMME

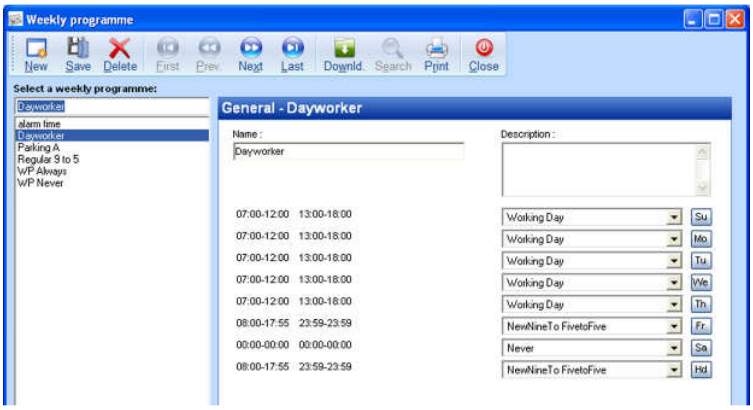
A Weekly Programme is made up of 8 Daily Programmes, one for each day of the week and an extra programme for holidays (Hd).

Notes:
By setting the option ‘Special days’ (see Tools/Options/General), two supplementary daily programmes may be added for 2 Special Days (S1 and S2) The dates for the Holidays and for the Special Days S1 and S2 are defined in the screen ‘Holidays’

Name: Name of displayed Weekly Programme.
May be edited.

Description: Free text

Table of Daily Programmes: The list of Daily Programmes making up this Weekly Programme is displayed - one for each day of the week (Su - Sa), holidays (Hd).



A new Weekly Programme can be defined by clicking **New**. For each day, select the required programme from the dropdown for that day. For each day, the times corresponding to the chosen Daily Programme are displayed in the left-hand column.

Clicking on the button showing the day name opens the corresponding Daily Programme screen. A new Daily Programme can be created there by clicking **New**.
Note: If Special Days option is used, two additional days can be defined.

Notes: Default Weekly Programmes - The two weekly programmes “WP Always” and “WP Never” are defined by default. Their names can be changed, but they may not be deleted nor modified.

HOW TIME ZONES CONTROL CARDHOLDERS, READERS, INPUTS & OUTPUTS AND REFLEXES

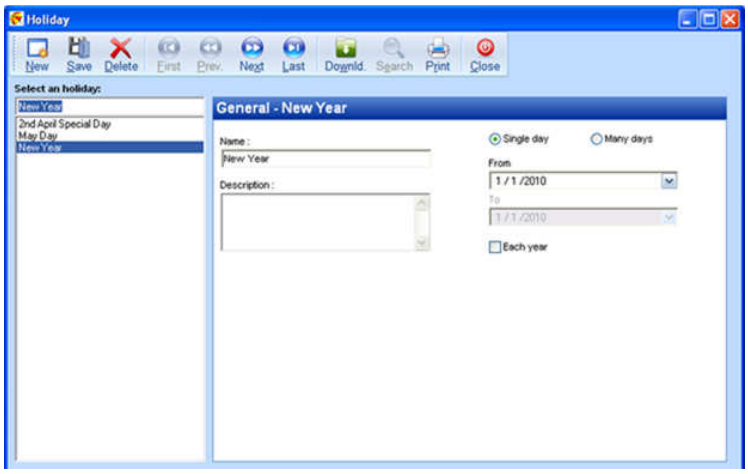
The following table shows the behavior of different items during the green and the red periods of their associated Weekly Program:

Item	'Green' periods	'Red' periods
Cardholder Access A W.P. attributed to a Cardholder defines when this cardholder may be granted access. It is attributed via his Access Group or his possible 'Personal Weekly Program' ('Cardholder/General' screen)	Access may be granted	Access denied
Readers A W.P. attributed to a reader defines its Access mode Rules. It is attributed via the 'Controller/reader-access mode' screen.	Security Level 1	Security Level 2
Alarm zones (Input Groups) or individual **Inputs** A W.P. attributed to an Alarm zone or an input defines when it is armed or disarmed. It is attributed via the 'Event handling programme' screen	Armed	Not armed
Output Relays A W.P. attributed to a relay defines when it is automatically activated. It is attributed via the 'Controller/output' screen	Activated	Not activated
Local reflexes A W.P. attributed to a local reflex defines when it can be triggered.It is attributed via the 'Controller/Local reflexes' screen	May be triggered	Not triggered
Global reflexes A W.P. attributed to a global reflex defines when it can be triggered. It is attributed via the 'Event handling/global reflexes' screen	May be triggered	Not triggered

3.4.3 HOLIDAY

The Holiday screen allows a list of dates to be defined on which the system should use a different set of Daily Programme rules. During these dates, rules of the 'Hd' programme (which is the 8th Daily Programme defined in the Weekly Programme) are enforced.

When the option 'Special days' is set (see Tools/Options/General), the field '**Day type**' appears. This allows which kind of day is being defined - either Holidays (Hd) or Special Day 1 or 2 (S1 or S2). During the dates defined as Special Day 1 or 2, rules of the 'S1' and 'S2' programmes (which are the 9th and 10th Daily Programme defined in the Weekly Programme) are enforced.



Screen opens on first existing Holiday in the list (Alphabetically).
New. To create a new Holiday

Name: Free text

Description: Free text

Single / multiple days: Use radio button to specify single or multi-day holiday

From: Use dropdown to open a calendar icon. Current calendar will show with 'Today' highlighted. Use the dropdown to display the calendar.
Select the required start date for the holiday.

To: Note: Only shown if multi-day holiday specified
Use dropdown to open a calendar icon. Select the required end date for the holiday

Each Year: Check this box if the holiday repeats on this date in all years

Day Type: Note: Only shown if Special Days option is used – defined in *Tools/Options/General*)

Days being defined as Holidays can be designated as "Special Day 1" or "Special Day 2".

3.5 ACCESS GROUP

Access Groups specify which doors are accessible, which Weekly Programmes are associated with each door, and each door's Crisis Level. By assigning each cardholder an appropriate Access Group, the user defines patterns for "who can go where and when". If a particular door is defined as accessible in the Access Group (i.e. with a ✓ for that reader), then during the 'green time' in that reader's associated Weekly Programme, a cardholder belonging to that Access Group may be allowed access.

Note: In order to reduce the overall number of separate Access Groups that must be defined, the system allows a cardholder to be associated with Multiple Access Groups.

Default Access Group: An access group "Anytime Anywhere" is defined by default. This provides permanent free access to all doors. Its name can be edited, but this group can neither be deleted nor modified.

Minimal authorization by default: When a new Access Group is created, all doors are selected and all are set to **X** (=no entry).

View: Checking the relevant box to show only Readers allowed for this Access group

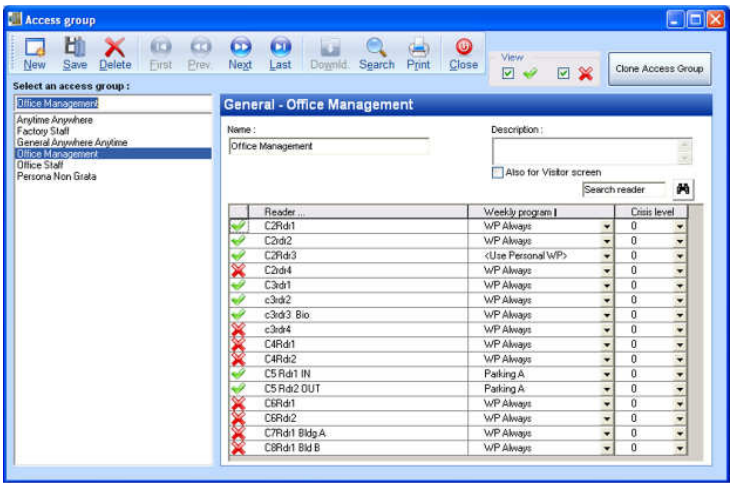
Clone Access Group button: Where a similar access group is needed, a copy of the selected access group can be created (named "copy of <selected AG>. . .). The clone can then be renamed and modified as required.

Name: Free text

Description: Free text

Also for Visitor screen: Check this box if this Access Group can be used for Visitors

Note: When LimitUserAG is set (in the .ini file), the check box 'Also for visitor' in this screen is disabled, as the LimitUserAG option has higher priority.



Search Field: To go directly to the entry for a particular reader, enter name or partial name and click search Icon. Readers matching the search string will be highlighted

Table of readers: Table shows all readers, with their associated Weekly programme and Crisis level.

Status indicator (✓or ×): Status of the selected reader in this access group can be toggled by clicking on the symbol (granted (✓) or denied (×))

Weekly Program: Use dropdown to select periods during which access is to be granted for that reader according to the 'green' periods set in the Weekly Programme.

Different error message in the log: Please note the difference in the error message that will associated to an access refusal in the following two cases:

	Reader …	Weekly Programme …	Error message if access denied:
✓	Rdr1 / Controller 1	WP Never	"Not authorized at this time"
×	Rdr2 / Controller 1	WP Always	"Reader not allowed"

3.6 DEPARTMENT

A department is an informative notion, which allows division of the site into various work areas, and allows a department to be chosen as a selection criterion to display and print reports. Departments may also be used for certain T&A functions.

Note on Time and Attendance T+: When the T+ Time and Attendance Option is used, all cardholders in a department share the same Daily Shift and Personal Contract. Thus, for each group of employees that must have its own definitions, separate departments are needed.

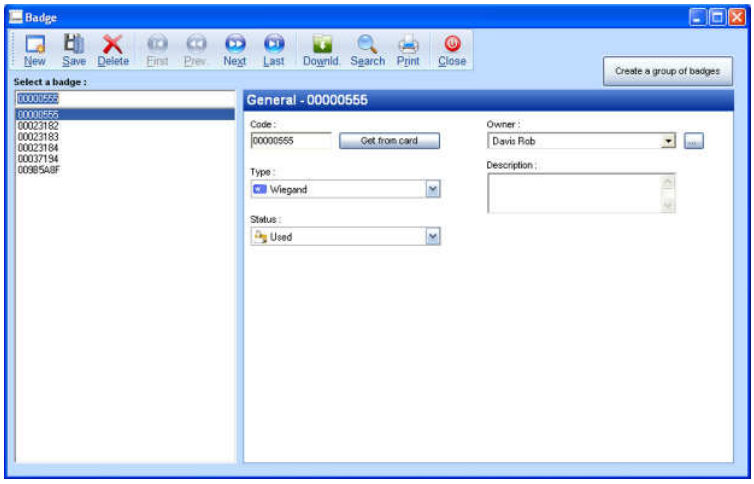
Name: Free text.
Departments are used for editing cardholders reports sorted by department and to associate cardholders with specific Personal Contracts.

Description: Free text

3.7 BADGE

This screen allows new badges to be registered in the system, and the parameters of new and old badges to be displayed and modified. An inventory of badges can be registered in the system so that they are ready to be issued.

Create a Group of Badges (Button): To create a group of badges, do not click on New, click on this button and open *Create a Group of Badges* screen. (see bellow)



Code: Enter the Card code, in decimal or hexadecimal. Leading zeros will be entered automatically to the default length of the card

Card Ranges: Where all the card codes start with a same prefix (for example **0500**12345, **0500**12346, etc.), a default 'range prefix' can be set (i.e. **0500**). The prefix chosen will then be automatically added at the beginning of the code when a new badge is created.
– See 'New' in the Principal Menu section of the *Options /General* screen.

Get from Card (Button): Opens *Get from Card* screen, for use if card code is not known. The code may be imprinted on the badge and human-readable, but generally, it is hidden. The Get from Card feature allows the code to be read from any reader (or one specific reader) and entered into the system without needing to be typed in

Type: Displays the Badge technology of the selected badge. When defining a new badge, the badge type default is defined in the 'Default badge technology' in the Principal Menu section of the *Options /General* screen

Where multiple badge types are in use, use the pull-down to choose the technology of this badge.

Note: Badge information (and therefore Access information regarding the cardholder who owns the badge) is only downloaded to controllers that support the selected badge technology.

Status: Use dropdown to change badge status if required.

- Free – default until badge is allocated to a cardholder
- Used – Badge is allocated to a user

- Cancelled – (Automatically invalid)
- Lost – (Automatically invalid)
- Stolen – (Automatically invalid)

Owner: Displays the name of the cardholder to whom the card is allocated.

If the badge is not yet allocated, <none> is displayed, followed by a list of Cardholders who do not yet have badges. Select the member of the list to whom this badge is to be allocated.

Click [...] to open the Cardholder screen and capture data for the new Cardholder or to edit information for the existing Cardholder.

Description: Free text

Note: The default Badge Length is be set **per Reader** in the *Reader/Miscellaneous/Badge format* screen.
This allows more than one format to be used within one installation.
However, all Readers on any particular controller **must** have the same length.

3.7.1 USING THE BADGE SEARCH

Displaying the list of all the allocated badges: Double click on the “Search” icon of the icon bar.

Performing a search on a specific type, status or owner

To find a badge from its type, status or owner:

- Click on the “Search” icon of the icon bar (or type “F10” key)
- Select the desired type, status or owner
- Click on the “Search” icon a second time
- If the badge is allocated, details of the badge will be displayed on the screen
- If no matching badge is found, the fields remain empty and the screen is greyed out
- Click on the “Search” icon to display the list of all the allocated badges

Searching a badge from all or part of its code: When using the “Search” icon, if the first characters of the code have been entered, the system will display all the badges that start with the desired sequence, after clicking the “Search” icon a second time.

Examples:

Code field	The system displays all the card codes with these attributes
32	Beginning with “32”
32%45	Beginning with “32”, which contain the characters “45”
_ _ _ _32_ _	Which contain the characters "32" at the 5th and 6th position

Note:

% will replace several characters

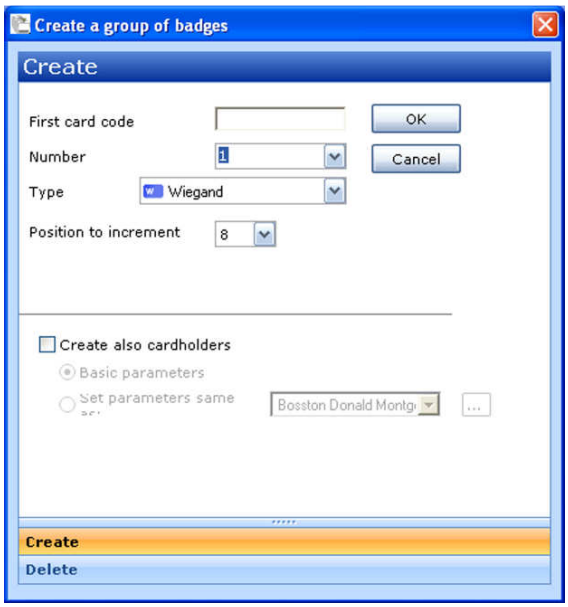
_ (underscore) will replace one single character

3.7.2 CREATE / DELETE A GROUP OF BADGES

This screen allows the creation and deletion of a group of badges using a single command. It is accessible via the *Parameter/Badge* or *Tools/Create a group of badges* menu.

3.7.2.1. CREATE A GROUP OF BADGES – CREATE TAB

Create a group of badges in a single command using this tab.



First card code: Type the code assigned to the first badge. Length (8-12 char) is as set in the *Reader/Miscellaneous/Badge Format* screen.

Note: A beginning card code common to all badges can be set in the *Tools/Options/General* screen.

Caution: The Create Group of Badges screen supports ONLY decimal codes – it cannot be used for Hexadecimal badges.

Number: Type or select the number of badges to create. The maximum number of badges depends on the dongle limitation.

Type: Choose the badge technology from the displayed list (Magnetic, Wiegand, etc.).

Note: The choice of reading technology will enable selective data download to the readers. Only data compatible with the selected technology will be downloaded to the readers.

Position to increment (between 1 and 8): Define the position of the digit to increment in the 8-digit sequence making up the code. This allows keeping a constant group of digits as code endings.

Example

First card code	Position to increment
12345789	5

The next code:

1234**6**789

Create cardholders also: Create simultaneously a group of badges and their associated badge holders, which will have:

- o Basic parameters: Valid employee parameters to whom the "Anytime Anywhere" access group is attributed
- o Set parameters same as: Specify the name of the badge holder whose parameters will serve as reference for the new badges

3.7.2.2 CREATE A GROUP OF BADGES – DELETE TAB

Remove a group of badges in a single command using this tab.

First card code: Type the 8-digit code assigned to the first badge (Only decimal codes are supported, not Hexadecimal)

Number: Type or select the number of badges to delete

Position to increment (between 1 and 8): Define the position of the digit to increment in the 8-digit sequence making up the code. This allows keeping a constant group of digits as code endings.

Example

First card code	Position to increment
12345789	5

The next code:

1234**6**789

Remove cardholders also: Delete a group of badges and at the same time, delete their corresponding cardholder records

Remove all non allocated badges: Delete all cards that are no longer allocated, i.e. temporary cards

Remove all deleted cardholders: Select to remove all deleted cardholders from the database

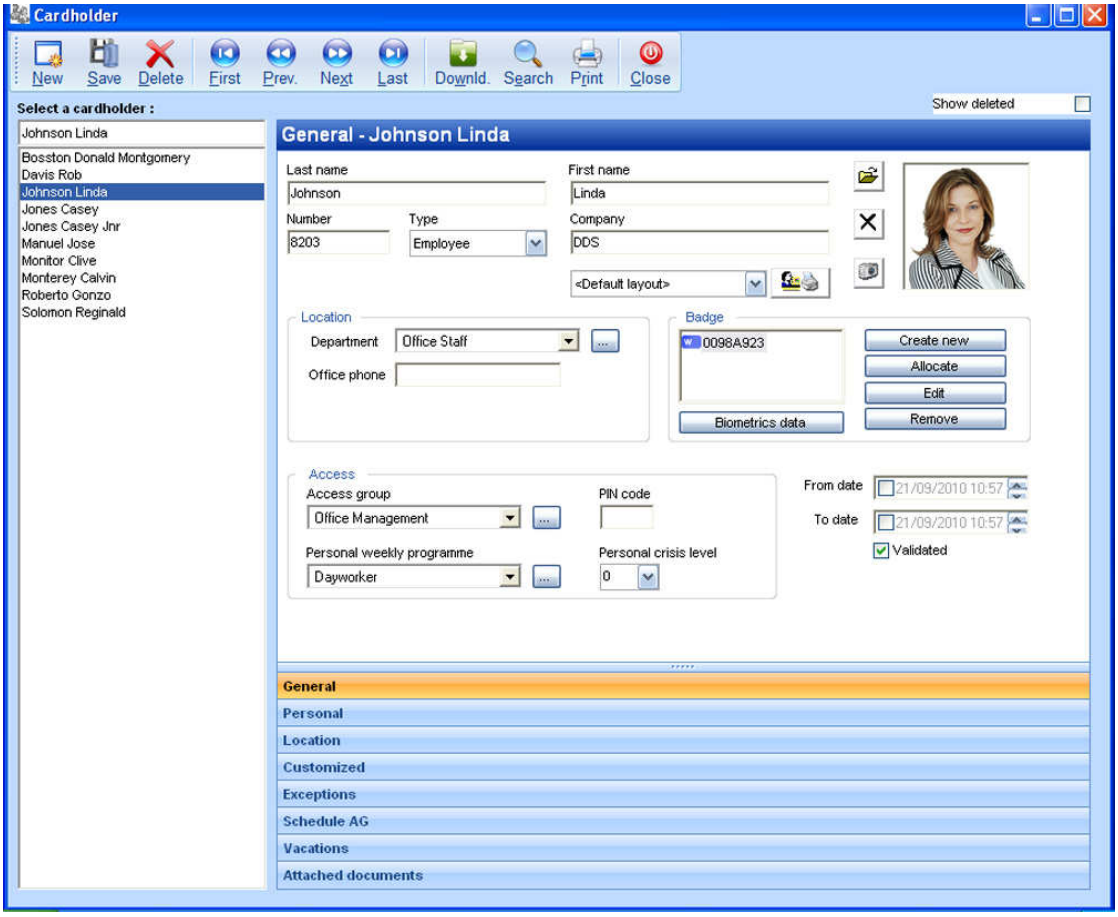
3.8 CARDHOLDER

Managing cardholders is the main purpose of the system. It allows:

- o Definition of cardholder's regular personal information (Name, Address, photos, car license number, etc.). The system also allows customized cardholder information to be defined
- o Definition of where, when and how cardholders may access to restricted zone.
- o Authorization of specific cardholders to perform operations such as arming/disarming alarm zones, turning on or off lights, operating air conditioning system, etc.

Cardholders' authorizations linked with access points are down-loaded to the controllers which manage these access points.

3.8.1 CARDHOLDERS / GENERAL



This screen records general information about the cardholder.

Cardholders can be registered in the system before badges are allocated to them. Records may be kept of badges that have been issued to cardholders and then withdrawn, such as visitors and employees who may have left the company.

The screen opens displaying the first record (alphabetically by Name).

Last Name: Free text

First Name: Free text

Number: An optional number identifying the cardholder in the organization.

Name and Number Settings: The sequence of cardholder records in the system is by 'Lastname:Firstname'. It is possible to override this and create cardholders with the same last and first name, by checking the **Allow duplicate name of cardholder's** field in the *Tools/Options/General* screen. Unique numbers must then be entered in the "Number" field for cardholders with identical names

Unique primary key: Where data is to be exchanged with external databases (through the *Cardholder Import* tool) , the Number field is used as the primary key for cardholder records.

Type: Use dropdown to choose Visitor, Employee, Guard, Deleted

Company: Free text

Badge Printing dropdown and Icon (only shown if this module is licensed.)

Select Layout dropdown: This will show <default layout> unless alternative layouts have been defined.

If alternative layouts are defined, use dropdown to choose layout.

Badge Preview/Print (button): This button accesses the *Badge Printing Preview* and *Badge Printing Design* screens

Location

Department: Use dropdown to select the cardholders department. Default is <none>. Click [...] to open the Department screen if a new department must be defined

Office Phone: Free text

Badge: Shows number and icon of type of badge allocated to this cardholder.

Create new: Click **Create new** to open the *Badge* screen, then either:

- Enter a new badge number in the **Code** field, or
- Click **Get from card** to register a new badge by reading it at a reader (Any unallocated badges read at any reader will be shown in the table) Choose a badge in the list and Click **OK** to allocate the selected badge

Allocate: To allocate a badge from existing unallocated badges

- Click **Allocate** to open the *Choose a card* screen
- Choose a card from the list of unallocated cards, and click on OK to return to the Cardholder screen

Note: If a 'non-allocated' card (i.e., card with ‘free’ status in the database) is passed (read) whilst this screen is open, then that card is automatically selected from the list of free cards. Thus the user does not need to search through all unallocated cards.

The selected badge will be shown in the new Cardholder’s record.

Edit: the *Badge* screen to allow information to be edited

Remove: Clears the current badge from the record so that a new badge can be allocated. The system allows only one card of a particular technology to one cardholder.

Access

Access group: Default is <Anytime Anywhere>

Use dropdown to assign the cardholder to a specific AG

Clicking [...] opens Access Group screen to see details and/or define a new AG

Assigning Multiple AGs to a cardholder: To assign Multiple Access Groups to the cardholder, click on <Multiple> in the dropdown list. The <Multiple> Access Groups screen will open.

If the cardholder has already been assigned Multiple Access Groups, then moving the mouse over <Multiple> will show a tooltip with the assigned Multiple Access Groups.

Note: The ini file entry ForceMultipleAG = 1 prevents the user from allocating individual Access Groups.

After modifying this entry to 1 and restarting the application, all cardholders who previously used only one AG are automatically redefined

PIN code: Enter 4-digit PIN code for this cardholder to use at a keypad reader

Personal weekly programme: Use dropdown to select Personal weekly programme for this cardholder. Default is <none>

To add a new Weekly Programme, click [...]

Using Personal Weekly Programmes: When a Personal Weekly Programme is selected for a cardholder, it affects only those readers for which, in the Access Group to which the cardholder belongs, the WP field option ‘<use personal WP>’ is selected

Personal crisis level: See ‘Access Groups’ in the full User Manual for a description of how to use Personal Crisis level

Validity

Controlling Badge Validity – From, To fields: These fields allow the user to set dates and times that define the period during which the badge may be used.

From date: Normally unchecked. If checked, the badge will not be usable before the date and time set. This allows the badge to ‘become’ valid at a future date.

To date: Normally unchecked. If checked, the badge will only be usable up to the date and time set. This allows the badge to ‘expire’ at a future date.

Validated: When the ‘From’ and/or ‘To’ date and time **are not used**, this checkbox allows to validate or not the cardholder in all the system.

When the ‘From’ and/or ‘To’ date and time **are used**, this checkbox is automatically updated according to the dates and times chosen.

Note: It is possible to inhibit automatically all cardholders who have not used their card during X days. This is done through the .INI file, Refer to this file description in the full manual for details.

Picture section

<Open File> Icon: Opens list of Identity Pictures – opens a standard Windows file search window, starting at current system location of the /Media/Portraits folder. Select the appropriate photo, and click Open to associate it with this cardholder. If the browse button is used and a picture from another location selected, then that picture will be copied into the Portraits folder.

<×>: Removes the association of the current picture with the cardholder. (Does not delete the picture in the Portraits file).

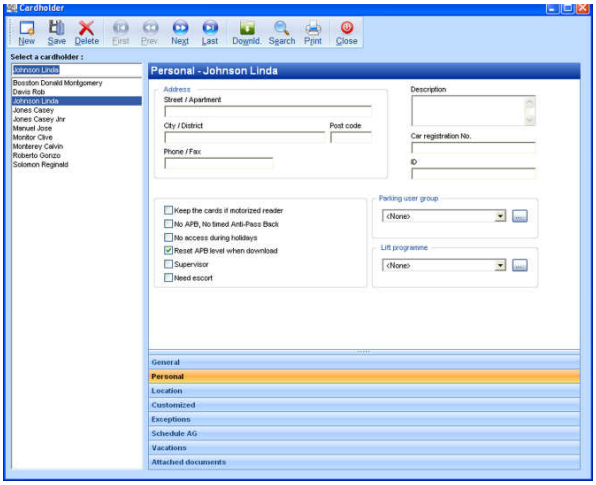
<camera icon>: Click on camera icon to use a camera connected to the PC to take a picture. The picture will be stored in the Portrait directory with a temporary name, which should be edited there before another picture is taken.

Show Deleted: Check this box to display all cardholder records including information on ‘deleted’ cardholders. If not checked, deleted records will not be shown.

Records can only be permanently removed from the system using the Delete Tab in the *Create a Group of Badges* screen

3.8.2 CARDHOLDERS / PERSONAL TAB

Allows Personal details to be stored about the Cardholder.



Address: Free text

Street/Apartment: Free text

City/District: Free text

Post Code: Free text

Phone/Fax: Free text

Keep the card if motorized reader:
Check if card to be retained on exit at Motorized reader/s

No APB, No timed Anti-PassBack: Check if these restrictions are not to be applied to this cardholder

No access during holidays: Check if access only allowed on working days

Reset APB when downloaded: Check if APB to be reset for this cardholder when Controllers are downloaded.

Note: This gives the Cardholder one access 'free' of APB checking. This allows re-synchronizing the APB level of the cardholder, when Global Anti-Passback is requested. The next access granted at any reader will update his APB level from this reader so that he can start a new APB sequence from this level.

Supervisor: Check this box if this cardholder has the status 'Supervisor' – This status will give him the following capabilities:

- Can escort a cardholder whose status is set to 'Need Escort'
- Can create a transaction with code 99 by presenting his card twice consecutively at a single reader, within 15 seconds. If a Global Reflex is triggered by this code, it will be executed.
- Can perform specific functions from readers equipped with keypad or DDS terminals. Examples: Arm or Disarm alarm groups, etc.

Need escort: Check this if this cardholder must be accompanied by a Supervisor.

Note: By checking both the 'Supervisor' and the 'Need Escort' parameters, a cardholder will be accepted without a second cardholder at a reader requiring 'escort'

Description: Free Text

Car registration No.: Free text

Note - Parking The cardholder's License No. is used by the Parking Module.

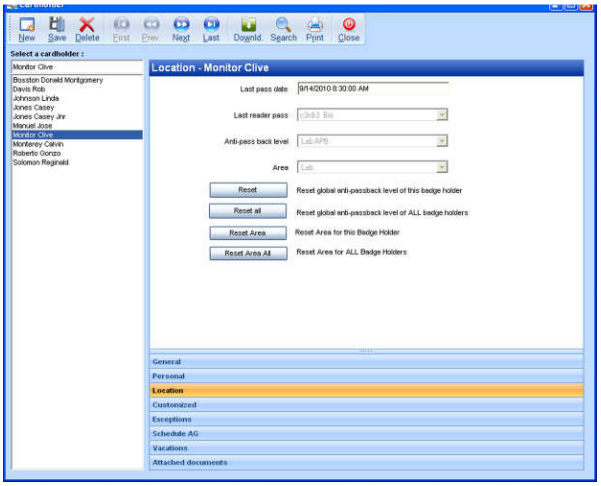
ID: Free text

Parking user group (only shown if Parking Module is used): <none> is default. If Parking Module is installed, use dropdown to select applicable group.

Lift programme (only shown if Lift Module is used): <none> is default. If the system controls lifts, use dropdown to select applicable programme.

3.8.3 CARDHOLDERS / LOCATION TAB

The Location facility allows a quick check on where a particular cardholder is, and allows that cardholder's location details to be reset if required.



Last pass date: Date and Time that this cardholder's badge was last read

Last reader pass: Reader at which the badge was read

Anti-Passback level: Current Anti-Passback level for this cardholder

Area: Current area for this cardholder

Reset button: Gives the Cardholder one access 'free' of APB checking. This is used to re-synchronize the APB level of the cardholder, when Global Anti-Passback is requested. The next access granted at any reader will update his APB level from this reader so that he can start a new APB sequence from this level.

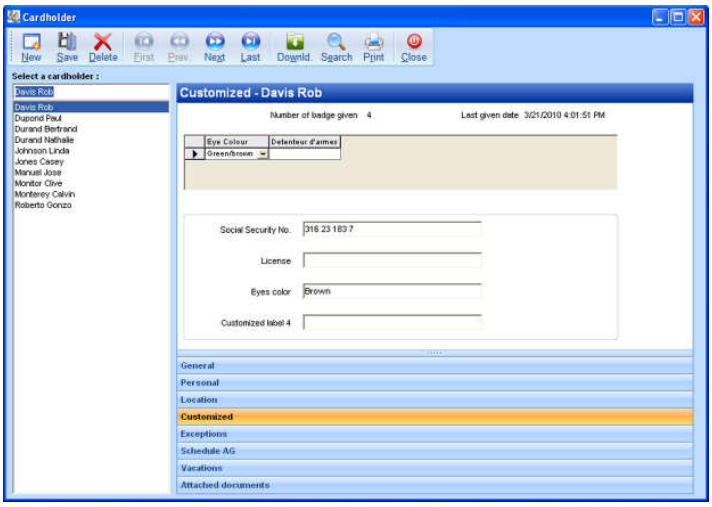
Reset all button: Resets the Global Anti-Passback level for all cardholders

Reset Area button: Resets the current Area for this cardholder to <none>. His current location will be updated by the next access granted at any reader.

Reset Area all button: Resets the current Area for all cardholders to <none>

3.8.4 CARDHOLDERS / CUSTOMIZED TAB

This screen shows details on the badge issue and allows defining customized area.



Number of badge given: Shows the 'issue number' of the cardholder's current badge (i.e. original badge will show as 1, each subsequent badge issued will increment the number)

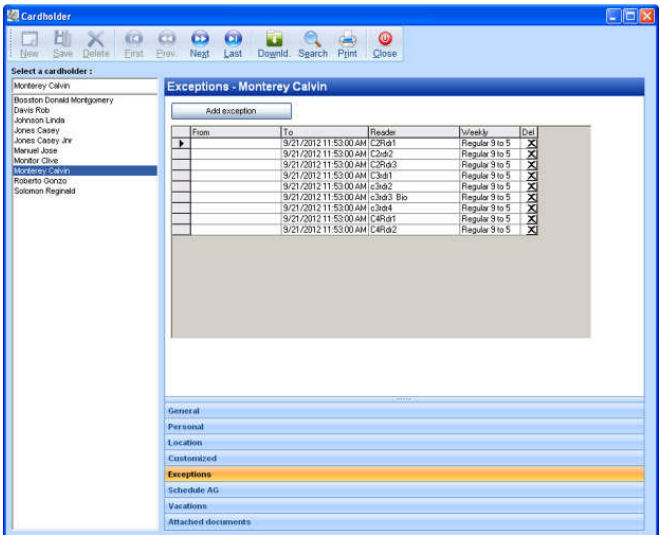
Last given date: Shows date and time that current badge was issued

Customized Fields Area: Area displays current contents of user-defined formatted data fields for this cardholder and allows data entry. Fields are defined in Customized Fields screen, see chapter 3.12.

Customized Labels Area: Four lines display current contents of user-labelled free text fields for this cardholder and allow data entry. "Labels are defined in Customized Labels screen, see chapter 3.12.

3.8.5 CARDHOLDERS / EXCEPTIONS TAB

This screen allows the user to allow or prevent access by the cardholder at one (or more) doors during pre-defined periods.



Select the cardholder whose rules are to be changed

Add exception button: Set the Start and End times and dates for the Exception, select a reader or a group of readers at which the Exception must be applied and select the Weekly Programme to be applied at the selected reader(s) for the duration of the Exception

Table of exceptions: List of all exceptions currently stored for this Cardholder

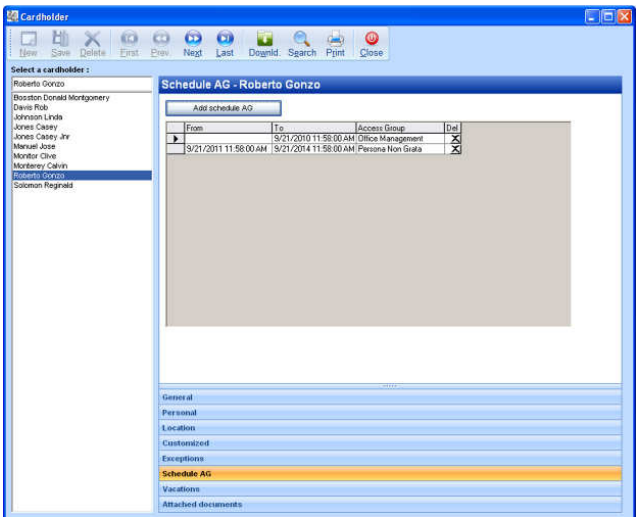
Del: Clicking on the X allows the selected Exception to be deleted

3.8.6 CARDHOLDERS / SCHEDULE AG TAB

This screen allows the cardholder to be assigned alternative Access Groups that will override their regular AG setting between specified dates. For each access during these periods, the cardholders regular AG is replaced by the scheduled AG specified here.

Add Schedule AG: Opens a window to define the start and end of a new Scheduled AG, and its applicable Access Group

From and To date: Set Start and End times and dates for the scheduled AG. Each field in the time and date can be selected with the mouse, and then adjusted with the up and down arrows



Note: If no Start and End dates and times are set, then this Scheduled AG will be put into effect immediately and stay in effect until deleted.

Access group: Use the dropdown to open a list of all existing AGs, and select the applicable AG

Table of schedule AGs: Shows all Scheduled AGs for the selected cardholder.

Any entry can be deleted by selecting the row (►) and clicking on the Delete symbol (✖).

A single entry showing no Start and End info means that an ongoing temporary AG has been assigned to the cardholder. No other entries will be accepted until this entry is deleted.

3.8.7 CARDHOLDERS / VACATIONS TAB

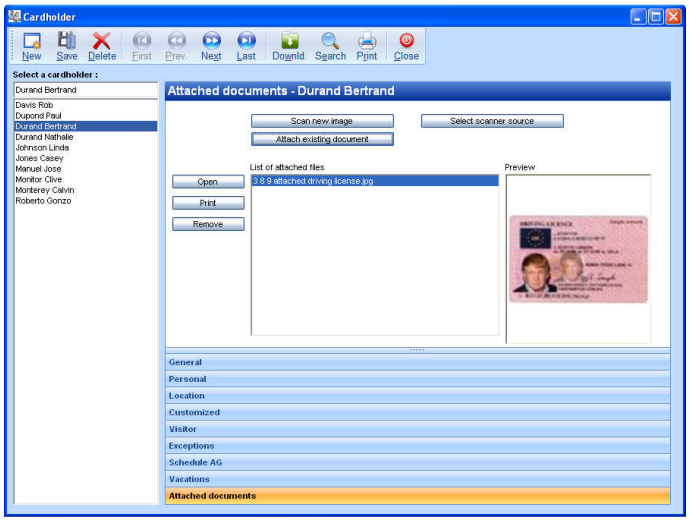
The Vacations screen is shown only when the T+ Time and Attendance Option is in use. See general manual for details.

3.8.8 CARDHOLDERS / ATTACHED DOCUMENTS

This screen allows images of scanned documents to be associated with specific Cardholders.

Scan New Image / Attach Existing Document: Opens a window allowing the user to name the image to be scanned or to give the location where an existing image may be found. In either case (new or previously stored image), a copy of the resulting file is stored in the application directory /Media/Docs

List of attached Files: A list of any files already associated with the employee highlighted in the navigation window is displayed.



The following actions are available:

Open / Print: Opens the selected image in a regular Windows Picture and Fax Viewer window, for viewing and/or printing.

Remove: Remove the selected file. The user has the option to simply remove the file from the cardholder's record, or to additionally delete it from the disk

Caution: Clicking the 'Remove' button **will always** remove the association of the document from the Cardholder record. There is no 'confirmation' of this action. Thus if the button is clicked in error, then the file must be re-associated using the 'Attach existing document' button.

3.9 VISITOR

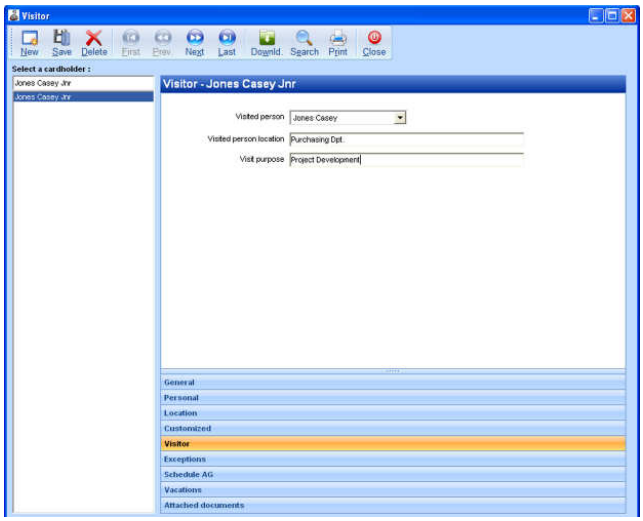
The Visitor screen is used to create new Visitor records and update Visitor information. It uses the normal Cardholder screen layout, but the type 'Visitor' is pre-selected.

The Visitor/Visitor tab (which can also be accessed from the Cardholder screen if the Cardholder type = 'Visitor' allows additional information about the Visitor to be captured.

Visited person: Dropdown – select the name of the person to be visited

Visited person location: Text field

Visit purpose: Text field



3.10 AUTHORIZATION LEVELS

An authorization level is a group of options and screens which can be 'viewed only' or 'viewed and modified' **only by users who belong to that level**.

Examples

- The site manager has access to all the information
- The parking lot attendant can only view cardholder details and modify information regarding parking
- The receptionist at the entrance of the building can only create visitors' badges and view details of cardholders, to look up phone numbers and current location of the person being visited

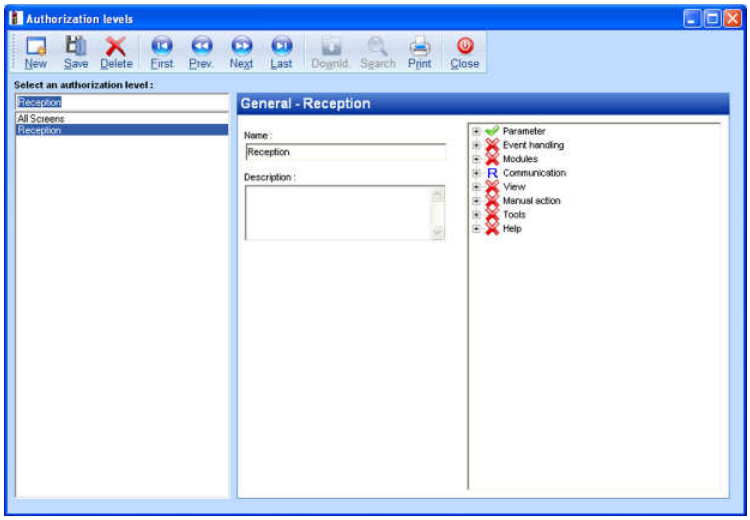
Once authorization levels are created using the Authorization Level screen, appropriate levels can be associated with any User who is being allocated a Username and Password in the *Parameter/User* screen.

A list of all Authorization Levels is shown.

When the screen is first opened, there is always a default Authorization Level set by the system called 'All Screens'. This Authorization Level's name can be changed, but its settings cannot be altered, and it cannot be deleted. Clicking **New** allows a new Authorization Level to be defined.

Name: Free Text

Description: Free text



Authorization tree: The authorization tree for the selected profile is displayed, showing the authorization for all screens. There are 3 possible authorization values for each screen or tab:

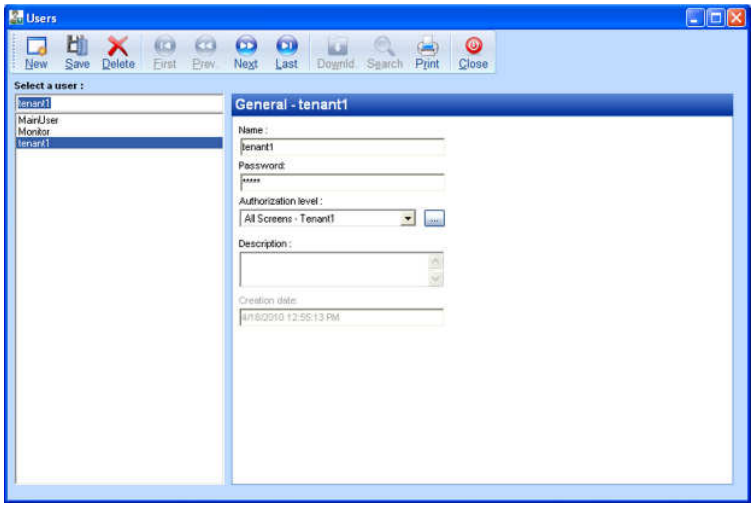
- o ✓ = full access allowed
- o **R** = read-only access
- o × = no access allowed.

Making a new Authorization level: Clicking on **New** allows a new Authorization level to be created. The tree of system screens is shown with all screens blocked except '**Parameter**', '**Log off**' and '**Exit**'. These are set to full access (✓**)** and cannot be changed. The user must then explicitly authorize each screen to which the members of this Authorization Level will have access, and whether the access is Read-only (**R**) or Full (✓).

3.11 USER

This screen registers Users, giving them User Names and passwords, and associates them with authorization levels which control what parts of the system they can access.

When the screen is first opened, there is always a default User set by the system (shown here as 'Main User'). This User's name can be changed, but will always have the Authorization Level 'All Screens' and cannot be deleted. Press **New** to create a new User



Name: User Name

Password: Enter the password for the new User. Passwords must be unique – no two users may share a password

Authorization Level: Use the dropdown to choose an

authorization level to associate with this User. Press […] to open the Authorization Level screen and create a new entry or modify an existing one.

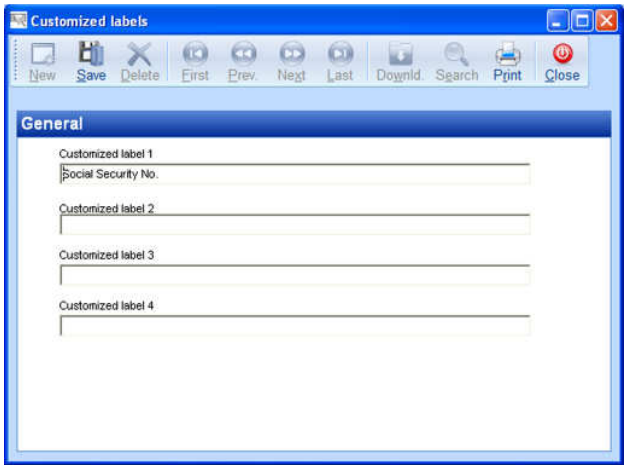
Description: Free text

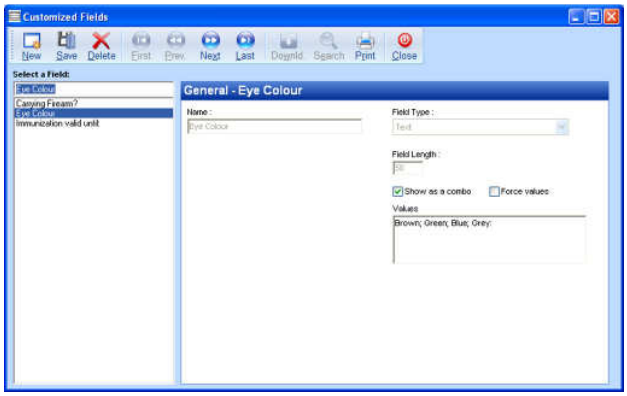
Creation Date: The system automatically completes this field

3.12 CUSTOMIZED LABELS AND CUSTOMIZED FIELDS

- *Customized Labels* – 4 **free-text** fields for which the user can customize the fieldname.

- *Customized fields* – additional **user-definable fields** for handling of information which can be checked/limited on entry.





4 EVENT HANDLING TAB

The Event Handling facilities allow programming, display, and management of alarms and user-defined processes. Alarm inputs may be armed/disarmed manually or according to user-defined time parameters. All events in the system can be handled through graphic representation: alarm inputs, output relays, processes and so on may be represented by icons/buttons. Icons may be positioned on maps and are automatically updated according to events as they occur. Processes may be activated automatically (Global reflexes) or triggered by the operator by clicking on their icons. (Refer to the complete User Manual of your installation CD for details on the “Event handling Menu)

The system provides powerful facilities to prepare fully customized dynamic displays all inputs and outputs, so that monitoring staff can use site maps to visualize the entire installation, view the status of all Inputs, see responses at Outputs, and follow the activation of reflexes that are set up in the system.

4.1 EVENT HANDLING PROGRAMME / ALARMS

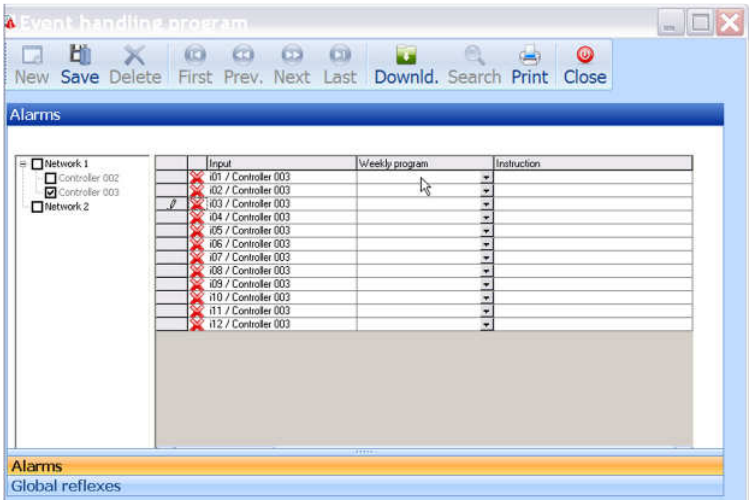
The Event Handling Programme tab allows the user to see the full list of Input Groups or individual Inputs in the system. These can be added or removed from the Event handling programme, and associated with a Weekly Programme.

When a weekly Programme is associated to an input, this input is armed during the green periods of its Daily Programme (set up in the Weekly Programme associated with it) and disarmed during the red periods.”

Messages (‘instructions’) can be associated with Individual Inputs, to be displayed in the Active Alarms screen if the Alarm associated with an Input is triggered.

Note: By default, all Input groups and Inputs are excluded from the Event handling programme. Thus an essential step in configuring an Alarm system is to include all required Input Groups in the Event Handling Programme.

View group of inputs’ radio button: Selecting the ‘View group of inputs’ button shows Input Groups (also called Alarm zones) instead of individual inputs:



This screen lists all Input Groups and allows each one to be associated with a Weekly Program. By selecting ✓, the

corresponding Input group is included in the Event Handling Programme, and will be armed during the 'green time' of the Weekly Programme with which it is associated, and disarmed during the 'red time'.

If the ✓ is selected without a Weekly Programme being specified and the definition saved, the Input Group will automatically be associated with the 'WP Always' weekly programme.

'View inputs' radio button: Selecting the 'View inputs' button shows individual inputs instead of Input Groups.

Navigation tree: The display can be limited to particular networks by checking or unchecking the relevant boxes. Information about individual controllers can be shown by clicking on the + symbol, and then only inputs on checked controllers will be shown.

Input: The Input column lists all the controller inputs for the networks selected in the Navigation window.

The two columns to the left of the Input column indicate:

- o whether the row has been selected (►), or whether it has been edited and not yet saved
- o The symbols ✓ and × indicate whether the input is currently associated with a Weekly Programme.
  If the value is toggled by clicking the ×, it will change to ✓. If it is then saved without first specifying a Weekly Programme, then it will automatically be associated with **WP Always**. If it is toggled from ✓ to **×,** then when it is saved, the Weekly Programme associated with it will be deleted.
- o Weekly Programme
  Shows the Weekly Programme associated with this input. The pulldown (▼) provides access to the list of all Weekly programmes, and an alternative may be selected.

Instruction: Free text. (e.g. 'call the police')

When alarms have occurred and are shown in the Active Alarms window, then clicking on a particular alarm will display the Instruction text in the Instruction pane

Selection symbol […]: Selecting the […] symbol for an Input opens the *Event Handling Program/Alarm Properties* window, allowing editing of the alarm properties linked with the Input.

Note:

A Weekly Programme may be attributed to an input either individually (using the 'View inputs' radio button) or, if the input belong to an input group, via this input group (using the 'View group of inputs' radio button). In the case that two different Programmes have been attributed to a same input, one via the 'view inputs' screen and the other via the 'view group of inputs' screen, then the Weekly Program *in the*

individual definition (via the 'view inputs' screen) will be applied. This can be useful when, within a group, an input is defective (for example, the detector connected to the input is broken): the Weekly Program 'never' will then be attributed to this individual input to prevent it giving alarms, even if the input group is armed.

Excepted for this case, and in order to avoid conflicts, it is recommended to attribute Weekly Programmes via Input Groups, and avoid using individual definitions.

4.2 EVENT HANDLING PROGRAMME / ALARM PROPERTIES WINDOW

This window opens from the Event Handling Programme window by clicking on the [...] symbol on the line of the selected Input, in the column to the right of 'Instruction'. It provides a convenient method for editing inputs and their alarm characteristics one at a time.

Input
Shows the name of the input currently selected. When this screen is first opened, the Input shown is whichever Input was being edited in the Event handling Programme window. Any of the Inputs shown in that window can be accessed here, by using the ↑ and ↓ arrows.

✓ and ×
Selecting these buttons allow the selected Input to be associated with a Weekly Programme, or de-associated from one. If associated with a Weekly Programme, then the Input will be armed during 'green' times, for that Weekly Programme.
If ✓ is selected, and no Weekly Programme is selected, then when the Input is updated (by clicking OK), it will automatically be associated with the Weekly Programme **WP always**.

Weekly programme: Shows the Weekly Programme currently associated with this Input. The dropdown allows an alternative weekly programme to be selected. Clicking the [...] symbol opens the *Weekly Programme* screen showing details of the associated Weekly programme, and allows a new weekly programme to be defined if required.

Instruction: Free text. (e.g. 'call the police')

When alarms have occurred and are shown in the Active Alarms window, then clicking on a particular alarm will display the Instruction text in the Instruction pane

Use only for reflex: Selecting this box indicates that the alarm is only to execute the process triggered by the input (defined in a Global Reflex) without raising or recording the alarm event in the journal history, and without being shown in the real-time log on the PC screen.

Priority: (0-9) Importance associated with this alarm

This is used in the Active Alarm Screen, where Alarms can be sorted by clicking on the Priority heading in the Alarms list

Process not repeated until confirmation: If a process is triggered by the input and if this box is selected, the process will be activated only the first time the input goes into alarm_ON state and not on subsequent alarms (as it is the case for a movement detector, for instance). To 'rearm' the process, the alarm must be confirmed.

↑ and ↓ arrows: Click to review the properties of the previous / next alarm.

Note: If any change was made, the system will ask whether to keep or discard the changes before moving to another input.

OK: Accept the parameters as entered.

Cancel: Discard changes and leave input definition as it was.

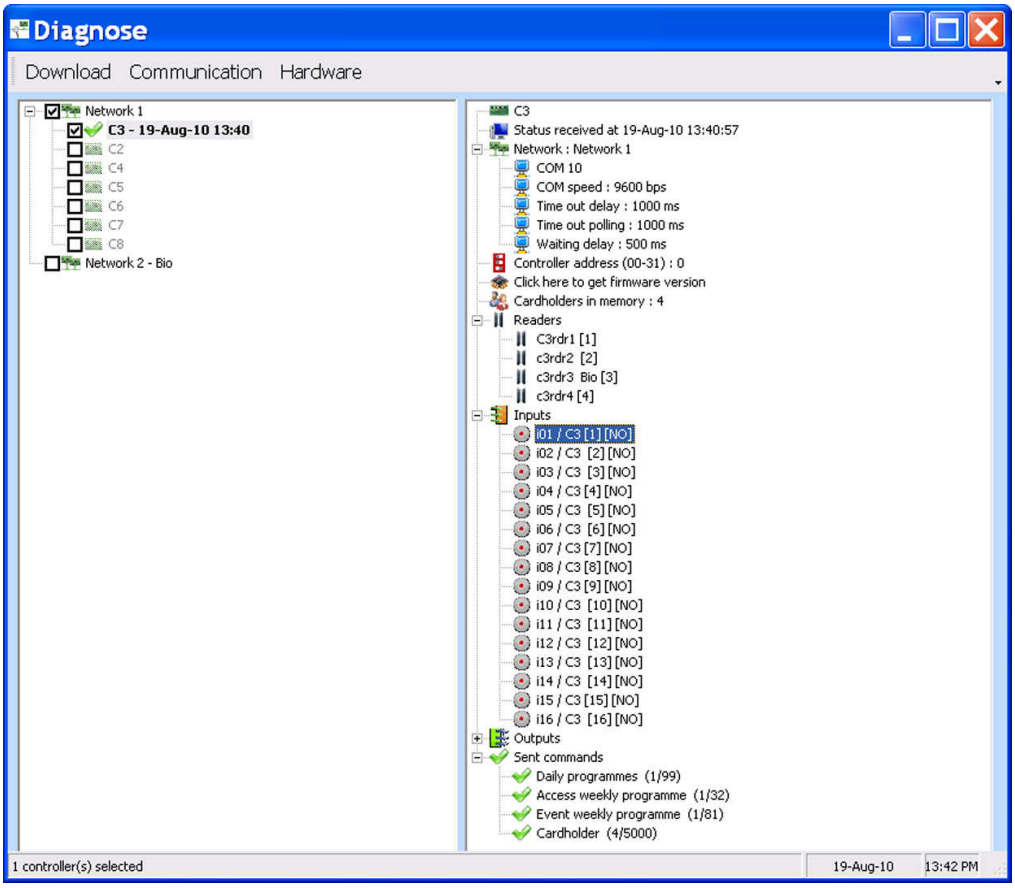
5 COMMUNICATION TAB

The Communication Tab provides the user with tools to monitor communication in the networks, see the status of all controllers and their attached hardware, reset and re-initialize them, and view /clear the current event log.

5.1 DIAGNOSTIC

The Diagnostic screen gives the user access to various Diagnostic tools.

5.1.1 DIAGNOSTICS – CONTROLLER INFORMATION



When a Controller is selected by clicking on the name, Controller details are displayed in the right-hand window

Note: If communications are not OK, then only the details that are stored in the database are shown.

- If communications is OK, then a green ✓ is shown, and the current Controller date and time are displayed.
  The system compares the Controller time with Application server time. If there is less than 5 mins difference, no change is made. Otherwise, the system automatically updates the Controller time. This change is made immediately, but is not shown until the next time the user clicks on this Controller.
- If communication cannot be established, then a red × is displayed.

The following controller details are shown:

Controller name: Name of this controller

Time and date: PC Time when these details were received

Network information: Expanding the Network entry (by clicking on the + symbol) shows the COM port used, the COM speed , the Timeout delay, the Time out polling and the Waiting delay

Controller Address: Physical address of the controller, as set in the HW DIP-switches

Firmware version button: Clicking this button gets the current firmware version information from the selected controller. The firmware version is given in dd/mm/yy format, followed by ROM information that may be used by hardware technicians.

Cardholders in memory: Shows the total number of cardholders for whom information is currently held in the selected controller

Readers: Expanding the Readers entry (by clicking on the + symbol) shows a list of the Readers associated with the selected controller.
Right-clicking on a reader gives the option of opening the associated Reader screen

Inputs: Expanding the Inputs entry (by clicking on the + symbol) shows the Inputs associated with the selected controller. Right-clicking on an Input gives the option of opening the associated Input screen

Outputs: As for Inputs

Pending: No. of commands not yet sent

Sent commands: Statistics are given for the commands sent to the selected controller. Right-clicking on a line gives the option of opening a screen with details of the selected command

5.1.2 DIAGNOSTICS / MENU

DOWNLOAD: Menu of the available downloads for the selected controllers

COMMUNICATION: Check the communication with the controllers

Check communications (all): One-time check of communications to all controllers

Check communications (selected): One-time check of communications to selected controller/s

Refresh every: Clicking on this option will set up an automatic Refresh cycle of all controllers selected in the left-hand window. A Refresh icon will appear at the bottom of the screen (see below)

HARDWARE: Allows checking the inputs/outputs status of the controller displayed in the right window

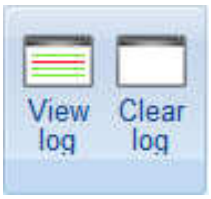
Refresh: One-time refresh

Refresh every: Clicking on this option will set up an automatic Refresh cycle of all items selected in the right-hand window. A Refresh icon will appear at the bottom of the screen (see below)

5.2 VIEW / CLEAR LOG

Clicking the View Log icon is a toggle which shows or hides the Log display window/s

Clicking the Clear Log icon erases all entries in the Log display window/s

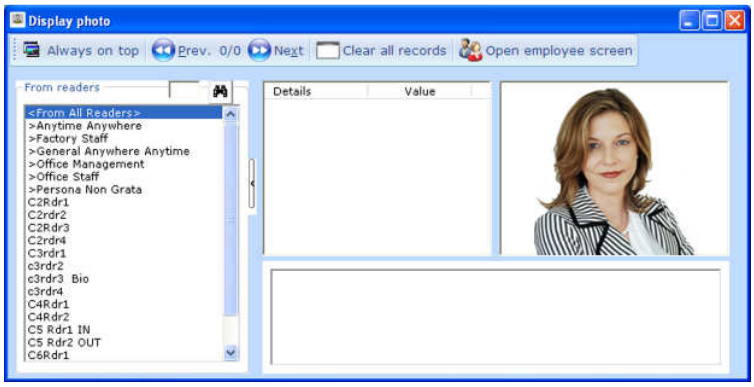


6 VIEW TAB

6.1 DISPLAY PHOTO

The Display Photo screen allows a user to view the pictures and the details of any cardholder/s as they pass their badge/s at specified reader/s.

The user can select whether the display is triggered by one or more readers.



Always on top: Clicking this button allows this screen to be viewed even if other windows are opened

Prev / Next: Shows the position of the currently-displayed record in the total number of records currently stored for viewing. Clicking on **Prev** or **Next** moves makes the previous or next record current. (max 100 records, then FIFO)

Clear All records: Clears all currently-stored records from the viewing buffer

From Readers: Select <From All Readers> or select the specific readers from which records are to be displayed. Selection is toggled on or off by clicking on the reader line.

Note: More than one reader can be selected.

Record Display: Details of the cardholder, their photo (if one is stored) and the latest reader log transaction are displayed. Double-clicking on the Photo field opens the corresponding Cardholder record.

7 TOOLS TAB

7.1 REPORT WIZARD

The Application incorporates a powerful report wizard. A wide variety of standard reports (which are all customizable for layout and content) are included in the system. Reports are compiled from the journal or from any other information of the database (parameters, events or modules).

Reports are generated in the language of the application. They can be displayed, printed or exported. The Preview function means that, at the press of a button, the user can see a how the report will look, to verify any step in the process of building it.

Four user-friendly screens lead the user, step by step, through the process: Select the required report, Select the data to be included, Filter the data to show only the required records and Organize the data (sorting and grouping).

7.1.1 REPORT WIZARD STEP 1/4 – REPORT SELECTION

The first screen of the report wizard allows the user to select an existing report or start defining a new one. It is accessible via the icon of the navigation bar or via the ‘’Tools‘’ menu.

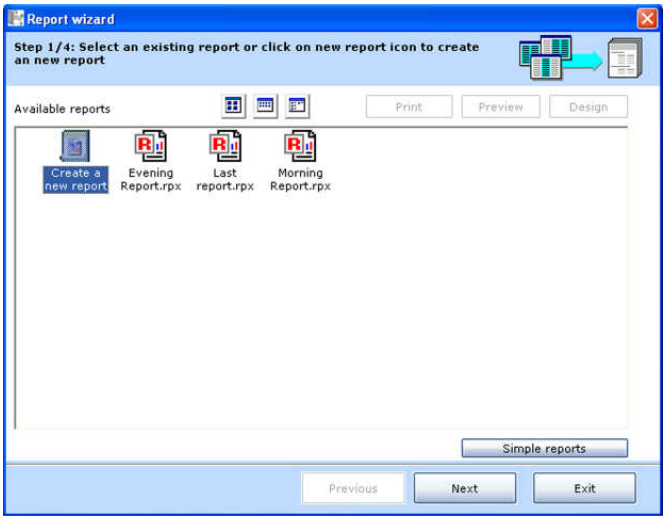
Available Reports: The ‘Available Reports’ window shows an icon to ‘Create a new report’, and icons for any other User-defined reports previously saved as x.rpx files. Double-clicking on any of the icons opens the *Report Wizard 2/4 screen - Data Selection* screen for the selected report. (The last report generated by using the Wizard is always shown in an icon called ‘Last Report.rpx’)

Command Buttons

Large icons, Small icons & List: The three blue icons allow the user to choose how the list of existing .rpx reports is shown.

Print: Click to print the selected report

Preview: Select a report in the list and click Preview to view the report as it will be printed



Design: Click to re-design the appearance of a selected report (for experienced users only)

Simple reports: Click to quickly create a standard journal report or to display a journal query.

Next: Click to go to the next step of the report wizard for the selected report

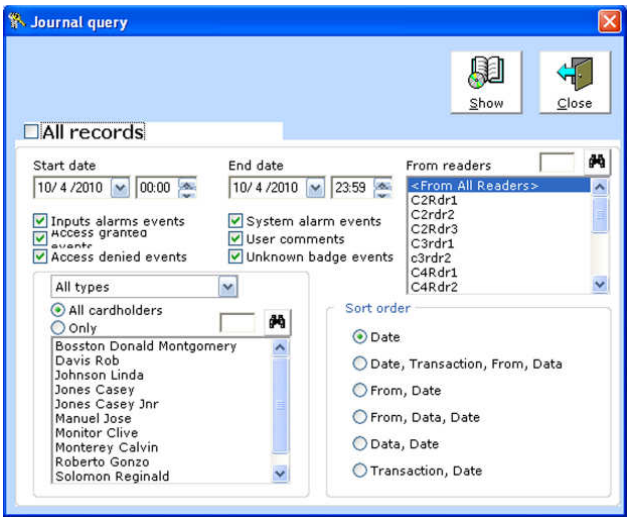
If no report is selected, the screen for a new report will automatically be opened.

Exit: Click to close the report wizard and go back to the main screen

7.1.1.1 REPORT WIZARD 1/4 - SIMPLE REPORTS

Selecting 'Simple Reports' in Report Wizard Screen 1 opens the Journal Query screen.

Fields



All records: The default setting has the 'All records' box selected. All options are greyed-out, and this setting produces a Journal Report for all transactions.

By unchecking the 'All records' box, the option fields are activated giving the view above, so that the user can choose parameters for the report.

Filtering and Sorting data: Select the data filtering criteria from the journal

- **By date**: Select the date and time for the start (Date dropdown opens a calendar, time edited by selecting hours or minutes and using ▲▼arrows). Default setting is 00:00 to 23:59, current day
- **By reader/s**: Select <All readers> or click on the specific reader(s) required
- **By events**: Check the events to keep: Inputs alarms, Access granted, Access denied, System alarm, User comments, Unknown badge
- **By type** – use 'All types' or select Visitor, Employee or Guard
- **By Cardholder/s**: Select 'All cardholders' or check 'Only' and click on the required cardholder(s)
- **Sort order**: Select the desired sort order of the data

Show: 'Show' displays all the records as a table, and in that display, 'Preview' allows the report to be viewed, printed or exported. Layout can also be edited if required.

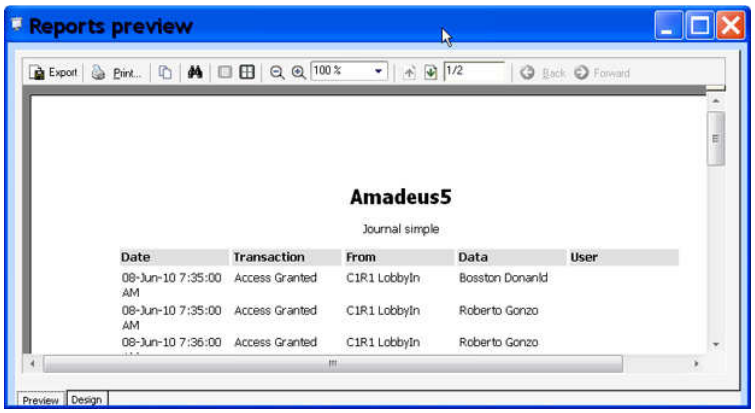
Close: Click to close the report wizard and go back to the main screen.

Users who do not have authorization to create a new report may still select a report and go directly to the *Data Filtering* screen to modify the report contents of existing reports.

7.1.1.2 REPORT WIZARD 1/4 - PREVIEW

This screen allows a screen preview of an existing report before printing and/or export.

Toolbar Buttons



Export: Opens the *Export* options window.

Selecting **Export** in the Preview screen opens the Export options window. Export Format available:

- RTF - Rich Text Format
- PDF - Portable Document Format (default)
- HTML - Hyper Text Markup Language
- XLS - Microsoft Excel
- TIF - Tagged Image Format
- TEXT

Print: Click to print after having specified printing parameters.

Copy this page to the clipboard: Click to copy the current page only

Find: Click to search for a specific word in the selected report.

Single Page, Multiple Page, Zoom Out, Zoom In

Zoom: Click to adjust the report preview.

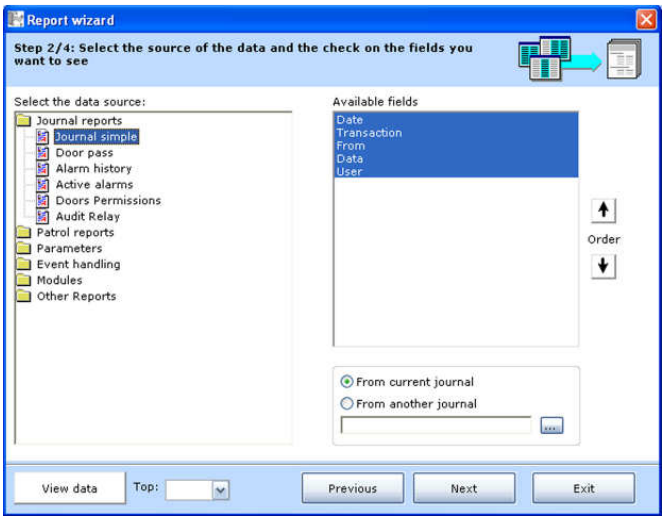
Previous Page, Next Page: Click to navigate in the report.

7.1.2 REPORT WIZARD STEP 2/4 – DATA SELECTION

The second step of the Report Wizard allows the user to select the fields to display in the report. For an existing report, the user can see the fields available for reporting, which fields are currently selected, and the display sequence. These parameters are easily modified.

If required, the user can also select a different source of data.

Note: This screen may be accessed at any time from any screen, by clicking on the "Print" button ("F11" function key). Depending on the screen from which the wizard was launched, the data fields available from that screen will be listed.



Left Window: Data sources list grouped in folders by type. Select the required one.

Right Window: Once the data source is selected in the left window, the corresponding list of available fields to display in the report is shown, with the default selected fields highlighted in blue. Fields can be toggled On and Off by clicking on them. Fields which are not selected at this stage will not appear in the remaining steps.

Buttons ↑ & ↓: Click on these buttons to move a selected field in order to re-order the columns in the report as required

Select the Journal from which to create the report: The Application allows the choice of the journal (period) of the report from current journal (by default) or from another journal (with "Access (mdb)" database ONLY). Select any other journal of the system by using the […] button, and specify its name and its directory

View data: Click on this button to preview the content of the data in table form; Click again on the "View data" button to quit this mode

Top: Enter the number of records or select from the dropdown the number of records to be processed for the View action.

By default, this field is set to 1000, which means only 1000 records will be processed. However, the maximum of records that can be processed by the View action is limited to 50,000. The Print action is also limited to 50,000 records.

In large installations this reduces the processing time, and requires the user to view a limited number rather than processing the whole database.

Previous: Click on this button to return at the previous step of the report wizard

Next: The 'Next' button is greyed out until there is a list of fields in the 'Available Fields' window. Click on this button to go to the next step of the report wizard

Exit: Click on this button to close the report wizard and go back to the main screen

Summary: Using the screen

To display the available data sources of a report type: Double-click on the required report type from the left window

To display the available fields of a data source: Click on the required data source from the left window; The right window shows the list of available fields, some of them already selected (in blue)

To select the required fields: Click on the available fields from the right window to change the default selection if required

To re-order the fields as required: Use the arrows button to move the fields. The "View data" toggle button may be used to preview the data of the report. After Previewing, click 'View data' to return to this screen.

To continue the creation or the modification of a report: Press the "Next" button to go to the next step of the report wizard

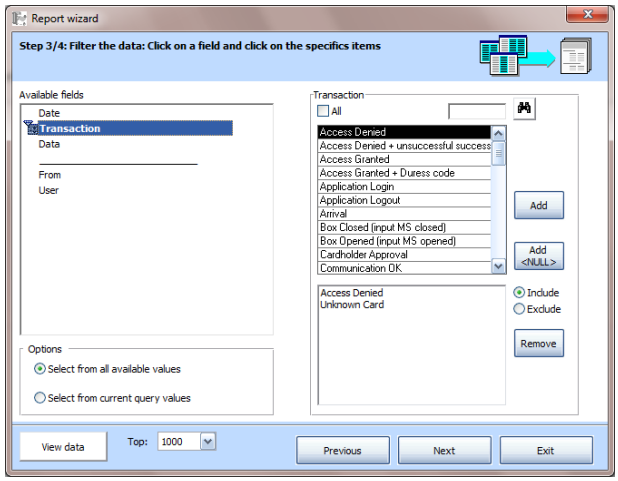
Notes:

1. The 'Journal Simple' report shows all transactions in the database (within the selected dates), including transactions of Deleted or Removed Cardholders.
2. The 'Door Permissions' report gives the Reader list showing, for each reader, who is allowed to access and when (i.e. by Weekly Programme). This report takes into account the Access Groups (standard and multiple), but it does NOT show Exception and ScheduleAG data.
3. Setting the ini file entry *ReportShowDeleted* = 1 adds the data type 'Deleted' to the choices for the **Door Pass** and **Door Permission** Reports. This allows the report to include transactions from deleted cardholders. (Remember – this works only for 'Deleted' cardholders. Once cardholders are 'Removed', their data cannot be shown on Door Pass and Door Permission reports.)
4. In the Door Pass report, the field 'Full name' is selected by default. This will use the cardholder name as held in the database when the report is created.
   If the user selects the field 'Name in Journal' to be used in the report, it must be kept in mind that the name that will appear in this field in the report will be the original name that was written in the Journal when the transaction occurred. In most cases, there will be no difference – this is only a consideration where the cardholder name (Last and/or First) is changed.

7.1.3 REPORT WIZARD STEP 3/4 – DATA FILTERING

The third screen of the report wizard allows fine tuning of the report by filtering the data.

Available Fields - Left Window: All the fields that were selected in the previous screen are shown. Fields to be printed appear first, and other fields, which may be used for filtering even though they will not appear in the report, are shown below a separating line.
Selecting any field in this window displays the corresponding data in the right-hand window. Depending on the type of data field selected, the right-hand window displays the type of filtering available.



Multiple Filters: Multiple filters can be defined. All fields that are already designated as filters are shown in bold, with a filter icon alongside it.
(Note: the filter icon appears only after clicking on another field on the left).

Removing a Filter: Any defined filter can be removed by selecting the field name in the Available Fields window (left), and clicking 'All' in the Right-hand window, and then clicking anywhere in the 'Available fields' window.

Available and Selected fields – Right Windows: The upper window shows all the **available values** of the field (that was selected on the left window), and the lower window shows the values that were added for filtering using the <Add> button.

Filtering buttons (Greyed out if '**All**' is selected)

- **Add –** Add the highlighted value to the filtering rule
- **Add <NULL>** - Select only records for which the value of the selected field is empty.
- **Include/Exclude Radio button –** Clicking these buttons toggles between including and excluding the records matching the selected data.
- **Remove –** Remove the selected value from the lower window.

Example (for Add <NULL>): In a 'All Cardholders' report, it is possible to filter by any field, e.g. Department, in order to select only cardholders that belong to a specific department. However, when we want to see in our report only people that do not belong to ANY department, i.e., their Department in Cardholder screen is set

to <None>, we need to select the 'Department' field on the left hand window click on the **Add <NULL>** button.

Select from all available values: All possible values of the selected field appear on the right window.

Select from current query values: Show on the right window the values of the selected field but only if they exist in the current journal. For example, if the current journal contains only events (transactions) of 'Access Grant' and 'Access Denied', then these two event types will be the only two values that would appear on the right when 'Transaction' field is selected on the left. All the other event types (unknown card, start of alarm, etc.) will not appear.

View data: Click on this button to preview the content of the data in table form. Click again on the “View data” button to quit this mode

Top: Enter the number of records or select from the dropdown the number of records to be processed for the View action.

Note: The dropdown gives numbers ‘All, 100, 200,… up to 50,000.

The maximum number of records that can be presented is 50,000.

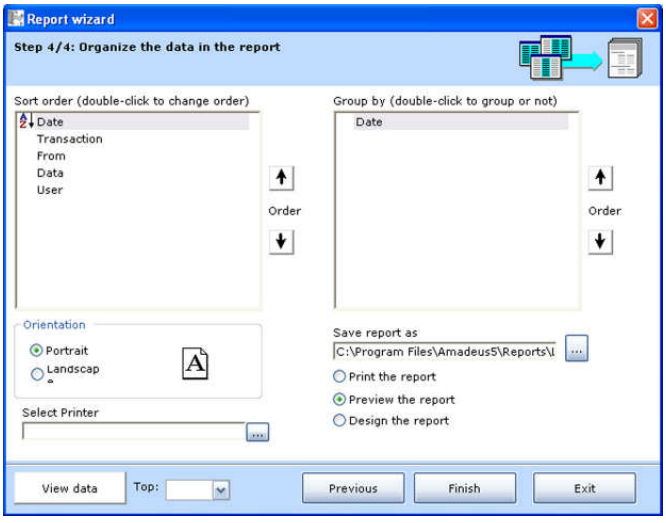
Previous: Click on this button to return at the previous step of the report wizard.

Next: Click on this button to go to the last step of the report wizard.

Exit: Click on this button to close the report wizard and go back to the main screen.

7.1.4 REPORT WIZARD STEP 4/4 – DATA ORGANIZATION

This last step allows data organization before preview for printing or exporting.



Sort Order window: By default, the records are sorted alphabetically by the first field from the list.

Double-clicking on a specific field will toggle between three possibilities:
Sorted A-Z, Sorted Z-A, Unsorted.
An icon will appear against any sorted field, showing the direction of the sort.

The name of any field selected for sorting will appear in the right-hand window

Grouping Window: All sorting fields show in the Grouping window. Double-clicking on any field in this window will result in a grouping the data in the report based on the contents of the field. An icon appears to show any fields designated as grouping criteria. By default, no field grouping is selected.

Buttons ↑ & ↓: Click on these buttons to classify the sorted fields or the grouped fields by importance order.

Orientation: Specify the report orientation (Portrait or Landscape)

Select Printer: Choose a printer for the report.

Save report as:
Allows the user to save the current report definition.
Default directory is the application **\Reports** directory
Default name is **Last report.rpx**.
(Thus if two successive reports are saved without changing the name, the earlier report definition will be over-written).

Once reports have been saved in the default directory, with the file extension .rpx, they will appear 'Available reports' window and can be re-used.

To store the report elsewhere, modify the location with […] button. (Such reports will NOT be available for re-use.)

Note: The .ini option 'Report folder' allows a workstation to store its own reports in a local folder.

Choice of Report destination: Print the report, Preview the report, Design the report

View data: Click on this button to preview the content of the data in table form Click again on the "View data" button to quit this mode

Top: Enter the number of records or select from the dropdown the number of records to be processed for the View action. (Max 50,000)

Previous: Click on this button to return at the previous step of the report wizard

Finish: Click to save the report and to execute the selected option
(Print the report, Preview the report or Design the report).

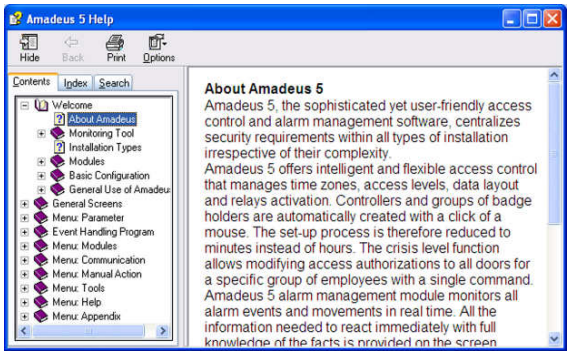
Exit: Click on this button to close the report wizard and go back to the main screen

7.2 OTHER AVAILABLE TOOLS

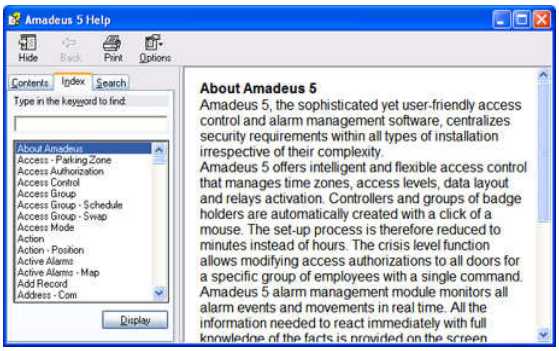
Different tools can be used for database, journal, cardholders or files management. Refer to the full manual for details.

8 HELP TAB

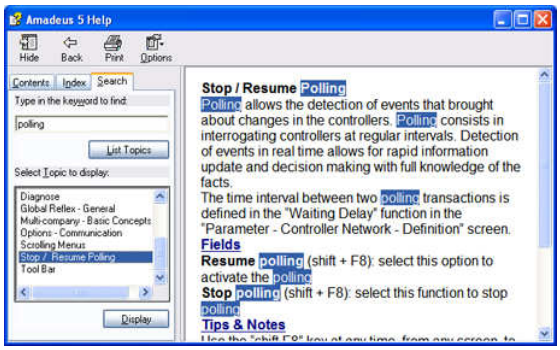
8.1 HELP CONTENTS


Amadeus 5 Help
Hide
Back
Print
Options
Contents
Index
Search
Welcome
About Amadeus
Monitoring Tool
Installation Types
Modules
Basic Configuration
General Use of Amadeu
General Screens
Menu: Parameter
Event Handling Program
Menu: Modules
Menu: Communication
Menu: Manual Action
Menu: Tools
Menu: Help
Menu: Appendix
About Amadeus 5
Amadeus 5, the sophisticated yet user-friendly access control and alarm management software, centralizes security requirements within all types of installation irrespective of their complexity.
Amadeus 5 offers intelligent and flexible access control that manages time zones, access levels, data layout and relays activation. Controllers and groups of badge holders are automatically created with a click of a mouse. The set-up process is therefore reduced to minutes instead of hours. The crisis level function allows modifying access authorizations to all doors for a specific group of employees with a single command.
Amadeus 5 alarm management module monitors all alarm events and movements in real time. All the information needed to react immediately with full

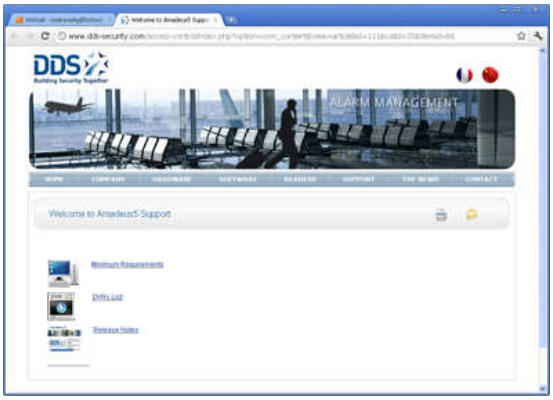
8.2 HELP INDEX


Amadeus 5 Help
Hide
Back
Print
Options
Contents
Index
Search
Type in the keyword to find:
About Amadeus
Access - Parking Zone
Access Authorization
Access Control
Access Group
Access Group - Schedule
Access Group - Swap
Access Mode
Action
Action - Position
Active Alarms
Active Alarms - Map
Add Record
Address - Com
Display
About Amadeus 5
Amadeus 5, the sophisticated yet user-friendly access control and alarm management software, centralizes security requirements within all types of installation irrespective of their complexity.
Amadeus 5 offers intelligent and flexible access control that manages time zones, access levels, data layout and relays activation. Controllers and groups of badge holders are automatically created with a click of a mouse. The set-up process is therefore reduced to minutes instead of hours. The crisis level function allows modifying access authorizations to all doors for a specific group of employees with a single command.
Amadeus 5 alarm management module monitors all alarm events and movements in real time. All the information needed to react immediately with full

8.3 HELP SEARCH


Amadeus 5 Help
Hide
Back
Print
Options
Contents
Index
Search
Type in the keyword to find:
polling
List Topics
Select Topic to display:
Diagnose
Global Reflex - General
Multi-company - Basic Concepts
Options - Communication
Scrolling Menus
Stop / Resume Polling
Tool Bar
Display
Stop / Resume Polling
Polling allows the detection of events that brought about changes in the controllers. Polling consists in interrogating controllers at regular intervals. Detection of events in real time allows for rapid information update and decision making with full knowledge of the facts.
The time interval between two polling transactions is defined in the "Waiting Delay" function in the "Parameter - Controller Network - Definition" screen.
Fields
Resume polling (shift + F8): select this option to activate the polling
Stop polling (shift + F8): select this function to stop polling
Tips & Notes

8.4 WEB



8.5 ABOUT

On startup, the 'About ' window is displayed – this presents the operating parameters (Identification,configuration limits and modules supported) set by the DDS dongle (plug).